KASPERSKY LAB

Kaspersky® Internet Security 6.0

MANUEL DE L'UTILISATEUR

KASPERSKY® INTERNET SECURITY 6.0

Manuel de l'utilisateur

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

http://www.kaspersky.fr/

Date d'édition: mars 2006

Sommaire

CHAPITRE 1. MENACES SUR LA SECURITE INFORMATIQUE

Le développement continu des technologies informatiques et leur introduction dans tous les domaines d'activités humaines s'accompagnent d'une augmentation du nombre de crimes visant les données informatiques.

Les organismes publics et les grandes entreprises attirent les cybercriminels. Ils cherchent à voler des informations confidentielles, à miner les réputations commerciales, à gêner le fonctionnement quotidien et à accéder aux données de ces différentes organisations. Ces diverses actions peuvent entraîner des dommages matériels, financières et moraux conséquents.

Les grandes entreprises ne sont pas les seules soumises au risque. Les particuliers peuvent également devenir des victimes. Les criminels, grâces à divers moyens, peuvent accéder aux données personnelles telles que des numéros de compte bancaire, des cartes de crédit ou des mots de passe, ils peuvent rendre un ordinateur totalement inutilisable ou prendre les commandes de celui-ci. Ces ordinateurs pourront être ultérieurement utilisés en tant qu'élément d'un réseau de zombies, à savoir un réseau d'ordinateurs infectés utilisés par les individus mal intentionnés en vue de lancer des attaques contre un serveur, de récolter des informations confidentielles ou de diffuser de nouveaux virus et chevaux de Troie.

Tout le monde est désormais conscient de la valeur des informations et de la nécessité de les protéger. Mais ces données doivent rester accessibles à un groupe défini d'utilisateurs (par exemple, les collègues, les clients ou les partenaires de l'entreprise). Il faut dès lors trouver un moyen de mettre en œuvre un système de protection complexe des données. Ce système doit tenir compte de toutes les sources envisageables de menaces (facteurs humains ou techniques, catastrophes naturelles) et doit reposer sur un ensemble de mesures de protection au plan physique, administratif et technique.

1.1. Sources des menaces

Les menaces qui planent sur les données peuvent émaner d'un individu ou d'un groupes d'individus ou peuvent provenir de phénomènes indépendants de toute intervention humaine. Sur la base de ces informations, les sources de menaces peuvent être scindées en trois groupes :

- **Facteur humain**. Ce groupe de menaces provient d'un individu qui possède un accès autorisé ou non aux données. Les menaces de ce groupe sont :
    - ***externes*** lorsqu'elles proviennent de cybercriminels, d'escrocs, de partenaires peu scrupuleux ou de structures criminelles.
    - ***internes*** lorsqu'elles impliquent un membre du personnel de l'entreprise ou le particulier qui utilise son ordinateur. Les actions des membres de ce groupe peuvent être préméditées ou accidentelles.
- **Facteur technique**. Ce type de menaces recouvre les problèmes techniques : matériel obsolète, mauvaise qualité des logiciels et du matériel utilisés pour traiter l'information. Tout cela entraîne la défaillance de l'équipement et, bien souvent, la perte de données.
- **Catastrophes naturelles**. Ce groupe contient tous les cas de forces majeures sur lesquels l'homme n'a aucun contrôle.

Il faut absolument tenir compte de ces trois catégories lors du développement d'un système de sécurité des données informatiques. Ce manuel traite uniquement de la source directement liée à l'activité de Kaspersky Lab, à savoir les menaces externes créées par un individu.

1.2. Propagation des menaces

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

Internet

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

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

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

base de registres système, le vol de données personnelles et l'installation de programmes malveillants.

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

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

Intranet

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

Courrier électronique

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

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

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

Média amovibles

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

Lorsque vous exécutez un fichier infecté par le code malicieux depuis un disque amovible, vous pouvez endommager les données sauvegardées sur votre ordinateur ou propager le virus sur d'autres disques de votre ordinateur ou des ordinateurs du réseau.

1.3. Types de menaces

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

Vers

Ce type de programmes malveillants se propage principalement en exploitant les vulnérabilités des systèmes d'exploitation. Les vers doivent leur nom à leur manière de passer d'un ordinateur à l'autre en exploitant le courrier électronique ainsi que d'autres canaux d'information. Cette technique permet à de nombreux vers de se diffuser à une très grande vitesse.

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

Virus

Il s'agit de programmes qui infectent d'autres programmes. Ils insèrent leur code dans celui de l'application ciblée afin de pouvoir prendre les commandes au moment de l'exécution des fichiers infectés. Cette définition simple permet d'identifier l'une des principales actions exécutées par les virus, à s'avoir *l'infection*.

Chevaux de Troie

Il s'agit d'applications qui réalisent diverses opérations sur l'ordinateur infecté à l'insu de l'utilisateur. Cela va de la destruction de données sauvegardées sur le disque dur au vol d'informations confidentielles en passant par le " crash " du système. Ces programmes malicieux ne sont pas des virus au sens traditionnel du terme (en effet, ils ne peuvent infecter les autres applications ou les données). Les chevaux de Troie sont incapables de s'introduire eux-mêmes dans un ordinateur. Au contraire, ils sont diffusés par des personnes mal intentionnées qui les présentent sous les traits d'applications « utiles ». Ceci étant dit, les dommages qu'ils occasionnent peuvent être bien plus sérieux que ceux produits par les attaques de virus traditionnelles.

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

Adwares

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

Logiciels espion

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

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

Riskwares

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

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

Jokewares

Ces programmes ne vont causer aucun dégât direct à votre ordinateur mais ils s'affichent des messages qui indiquent que des dégâts ont déjà été commis ou qu'ils seront commis sous certaines conditions. Ces programmes préviennent souvent les utilisateurs d'une menace inexistante telle que le formatage du disque dur (alors qu'aucun formatage n'est exécuté), découvrent des virus dans des fichiers sains, etc.

Rootkit

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

Autres programmes dangereux

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

Attaques de pirates informatiques

Les attaques de pirates informatiques sont le fait d'individus mal intentionnés ou de programmes malveillants qui veulent s'emparer

d'informations sauvegardées sur l'ordinateur de la victime, mettre le système hors service ou obtenir un contrôle total sur les ressources de l'ordinateur. Vous trouverez une description détaillées des attaques bloquées par Kaspersky Internet Security dans la section Liste des attaques de réseau découvertes.

Certains types d'escroquerie via Internet

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

La n**umérotation vers un site Internet payant** est un type d'escroquerie qui repose sur l'utilisation non autorisée de sites Internet payants (bien souvent, des sites à contenu pornographique). Les programmes installés par l'individu mal intentionné (les dialers) ouvrent une connexion par modem entre votre ordinateur et le numéro payant. Dans la majorité des cas, le tarif de cet appel est très élevé, ce qui se traduit par une lourde facture de téléphone pour l'utilisateur.

Publicités envahissantes

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

Courrier indésirable

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

Kaspersky Internet Security identifie et bloque ces différentes menaces en exploitant deux méthodes :

- *méthode réactive* : cette méthode repose sur la recherche des objets malicieux à l'aide d'une base des signatures des menaces qui est actualisée en permanence. Cette méthode requiert au moins une infection pour ajouter la signature de la menace dans la base et diffuser la mise à jour.
- *méthode proactive* : au contraire de la méthode réactive qui repose sur l'analyse du code de l'objet, l'analyse proactive implique l'analyse du comportement de l'objet dans le système. Cette méthode permet d'identifier de nouvelles menaces qui ne sont pas encore reprises dans les bases.

En adoptant ces deux méthodes, Kaspersky Internet Security peut garantir la protection sophistiquée de votre ordinateur contre les nouvelles menaces ou les menaces inconnues.

Attention !

Dans ce manuel, le terme « virus » désignera aussi bien les programmes malveillants que les riskwares. Le type de programme malveillant sera précisé au besoin.

1.4. Signes d'une infection

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

- Des messages, des images ou des sons imprévus se manifestent ;
- L'ouverture et la fermeture inattendue du lecteur de CD/DVD-ROM;
- Le lancement aléatoire d'une application quelconque sans votre intervention;
- L'affichage d'un avertissement relatif à la tentative réalisée par un programme de se connecter à Internet bien que vous n'ayez pas lancé cette action,

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

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

- Vos amis ou vos connaissances parlent de vos messages alors que vous ne leur avez rien envoyé ;

- Votre boîte aux lettres contient énormément de messages sans objet et sans adresse d'expéditeur.

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

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

- Gel et échecs fréquents dans le fonctionnement de l'ordinateur ;
- Lenteur au moment du lancement des logiciels ;
- Impossibilité de charger le système d'exploitation ;
- Disparition de fichiers et de répertoires ou altération de leur contenu ;
- Requêtes fréquentes vers le disque dur (la petite lampe sur la tour clignote fréquemment) ;
- Le navigateur (par exemple, Microsoft Internet Explorer) « plante » ou se comporte bizarrement (ex. :impossible de fermer les fenêtre du logiciel).

Dans 90% des cas, ces symptômes sont causés par des problèmes matériels ou logiciels. Même si ces symptômes ne sont pas nécessairement la manifestation d'une infection, il est fortement conseillé de réaliser une analyse complète de l'ordinateur (cf. point 5.4, p. 62) selon les paramètres définis par les experts de Kaspersky Lab dès qu'ils se manifestent.

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

Si vous remarquez que votre ordinateur a un comportement suspect :

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

du disque de secours de Microsoft Windows que vous avez créé au moment de l'installation du système d'exploitation.

4. Avant d'entamer quoi que ce soit, réalisez une copie de votre travail sur une disquette, un CD, une carte Flash, etc.
5. Installez Kaspersky Internet Security, si cela n'a pas encore été fait.
6. Actualisez les signatures des menaces (cf. point 5.8, p. 65) du programme. Dans la mesure du possible, réalisez cette opération depuis l'ordinateur sain d'un ami, d'un cybercafé ou du travail. Il est en effet préférable d'utiliser un autre ordinateur car si le vôtre est bel et bien infecté, sa connexion à Internet permettra plus que probablement au virus d'envoyer des informations importantes à une personne mal intentionnée ou de se propager en envoyant une copie à tous les contacts de votre carnet d'adresses. C'est pour cette même raison qu'il est toujours conseillé de déconnecter votre ordinateur d'Internet si vous soupçonnez une infection. Il est possible également d'obtenir les mises à jour sur une disquette ou sur un disque en s'adressant à Kaspersky Lab ou à l'un de ses distributeurs. Dans ce cas, la mise à jour s'effectue localement.
7. Définissez le niveau de protection défini par les experts de Kaspersky Lab.
8. Lancez l' analyse complète de l'ordinateur (cf. point 5.4, p. 62).

1.6. Préventions des infections de votre ordinateur

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

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

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

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

- Installez sans plus attendre Kaspersky Internet Security.

- Actualisez (cf. point 5.8, p. 65) régulièrement les signatures des menaces livrées avec le logiciel. Réalisez cette opération plusieurs fois par jour en cas d'épidémie (les bases antivirus sont publiées sur les serveurs de mises à jour de Kaspersky Lab immédiatement dans ce genre de situation).
- Configurez les paramètres de protection recommandés par les experts de Kaspersky Lab. La protection en temps réel est active dès le démarrage de l'ordinateur et complique la tâche des virus qui souhaiteraient l'infecter.
- Appliquez les paramètres recommandés par les experts de Kaspersky Lab pour l'analyse complète de l'ordinateur et prévoyez son exécution au moins une fois par semaine. Si vous n'avez pas encore installé Anti-Hacker, faites-le pour protéger votre ordinateur pendant que vous êtes connecté à Internet.

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

- Recherchez la présence d'éventuels virus dans tous les disques amovibles (cf. point 5.6, p. 63) (disquettes, CD, cartes Flash, etc.) avant de les utiliser.
- Traitez les courriers électroniques avec prudence. N'ouvrez jamais les fichiers que vous recevez par courrier électronique si vous n'êtes pas certain qu'ils vous sont bel et bien destinés, même s'ils ont été envoyés par vos connaissances.
- Soyez attentif aux données reçues depuis Internet. Si un site Internet vous invite à installer une nouvelle application, veillez à vérifier son certificat de sécurité.
- Lorsque vous copiez un fichier exécutable depuis Internet ou depuis un répertoire local, analysez-le avec Kaspersky Internet Security avant de l'ouvrir.
- Soyez prudent dans le choix des sites que vous visitez. En effet, certains sites sont infectés par des virus de script dangereux ou par des vers Internet.

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

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

Règle N°4 : *Ne croyez pas les canulars présentés sous la forme d'un message évoquant un risque d'infection*.

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

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

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

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

- Réalisez régulièrement des copies de sauvegarde de vos données. Celles-ci vous permettront de restaurer assez rapidement le système en cas de perte de données. Conservez en lieu sûr les CD et les disquettes d'installation ainsi que tout média contenant des logiciels et des informations de valeur.
- Créez un disque de secours (cf. point 16.9, p. 263) qui vous permettra, le cas échéant, de redémarrer l'ordinateur à l'aide d'un système d'exploitation « sain ».

Règle N°9 : *Consultez régulièrement la liste des programmes installés sur votre ordinateur*. Pour ce faire, vous pouvez utiliser le point **Ajouter/Supprimer des programmes** dans le **Panneau de configuration** ou ouvrez simplement le répertoire **Programmes**, le dossier de démarrage automatique. Vous pourrez ainsi découvrir les logiciels qui ont été installés sur votre ordinateur à votre insu, par exemple pendant que vous utilisiez Internet ou installiez un autre programme. Certains d'entre eux sont probablement des riskwares.

CHAPITRE 2. KASPERSKY INTERNET SECURITY 6.0

Kaspersky Internet Security 6.0 représente la nouvelle génération de solution de protection des données.

Ce qui différencie Kaspersky Internet Security 2006 des produits existants, et notamment des autres logiciels de Kaspersky Lab, Ltd., c'est l'approche complexe adoptée pour protéger les données de l'utilisateur. Ce logiciel assure la protection contre tous les types de menaces existantes à l'heure actuelle, mais également contre les menaces à découvrir, ce qui est tout aussi important.

2.1. Nouveautés de Kaspersky Internet Security 6.0

Kaspersky Internet Security 6.0 représente une approche révolutionnaire dans le domaine de la protection des données. Tout d'abord, ce programme regroupe toutes les fonctions de tous les logiciels de la société au sein d'une solution de protection complexe. Ce programme vous protégera non seulement contre les virus, mais également contre le courrier indésirable et les attaques des pirates informatiques. Les nouveaux modules offrent également une protection contre les menaces inconnues, depuis le phishing jusqu'à la dissimulation d'activité malveillante.

Il n'est plus indispensable d'installer plusieurs logiciels afin d'assurer la sécurité complète. Il suffit simplement d'installer Kaspersky Internet Security 6.0.

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

Examinons maintenant en détails les nouveautés de Kaspersky Internet Security 2006.

Nouveautés au niveau de la protection

- Désormais, Kaspersky Internet Security vous protège non seulement contre les programmes malveillants connus, mais également contre ceux qui ne le sont pas encore. Le composant de défense proactive (cf. Chapitre 10, p. 122) constitue le principal avantage du logiciel. Il analyse

le comportement des applications installées, est à l'affût de changement dans la base de registre, surveille l'exécution des macros et lutte contre les menaces dissimulées. Le composant exploite un module d'analyse heuristique qui permet d'identifier divers types de programmes malveillants. Il maintient un historique de l'activité malveillante pour repousser les actions néfastes et rétablir le système à son état antérieur à l'intervention du code malveillant.

- Protection contre les programmes de dissimulation, les dialers vers des sites Web payant, blocage des fenêtres pop up, des bannières publicitaires et des scripts dangereux téléchargés depuis des pages Web et identification des sites de phishing.
- Modification de la technologie de protection des fichiers sur l'ordinateur de l'utilisateur : il est désormais possible de réduire la charge et d'augmenter la vitesse de l'analyse des fichiers. Ce résultat est obtenu grâce au recours aux technologies iChecker et iSwift et en analysant uniquement les nouveaux fichiers ou ceux qui ont été modifiés (cf. point 7.2.1, p. 93). Ainsi, les fichiers qui n'ont pas été modifiés depuis la dernière analyse peuvent être ignorés.
- La recherche de virus est désormais soumise à votre utilisation de l'ordinateur. L'analyse est gourmande en temps et en ressources système, mais l'utilisateur peut poursuivre son travail. Si l'exécution d'une tâche quelconque requiert plus de ressources système, la recherche de virus sera suspendue jusqu'à la fin de cette tâche. L'analyse reprendra là où elle avait été interrompue.
- L'analyse des secteurs critiques de l'ordinateur, ceux dont l'infection entraînerait des conséquences irréversibles, est reprise dans une tâche séparée. Vous pouvez configurer cette tâche de telle sorte qu'elle soit lancée à chaque démarrage du système.
- La protection du courrier sur l'ordinateur de l'utilisateur, tant contre les programmes malveillants que contre le courrier indésirable, a été considérablement améliorée. Le logiciel analyse n'importe quel message et recherche les messages non sollicités dans le flux de messagerie des protocoles suivants :
    - IMAP, SMTP et POP3 quel que soit le client de messagerie utilisé ;
    - NNTP (recherche de virus uniquement), quel que soit le client de messagerie ;
    - MAPI, HTTP (dans le cadre des plug-ins intégrés à Microsoft Office Outlook et TheBat!).
- Des plug-ins permettant de configurer directement la protection du courrier contre les virus et le courrier indésirable dans le système de

messagerie ont été intégrés aux clients de messagerie les plus connus comme Microsoft Office Outlook, Microsoft Outlook Express et The Bat!

- L'entraînement d'Anti-Spam s'opère sur la base des messages de votre boîte aux lettres, ce qui permet au programme de tenir compte des particularités de votre travail et de configurer en souplesse l'identification des messages non sollicités. L'algorithme de Bayes et au cœur de cet entraînement. Vous pouvez constituer des listes "noires" et "blanches" d'expéditeurs ainsi que des listes d'expressions clés qui permettront d'identifier le courrier indésirable.

  Anti-Spam exploite également une base de données de phishing. Cette base permet de rejeter les lettres dont l'objectif était d'obtenir des informations confidentielles à caractère financier.

- Le logiciel filtre le courrier entrant et sortant, suit et prévient la propagation des attaques de réseau et permet de travailler en mode "furtif".

- Lors d'une connexion à un réseau, vous pouvez définir les réseaux fiables à 100% et ceux avec lesquels il faut faire très attention.

- Elargissement de la fonction de notification de l'utilisateur (cf. point 16.10.1, p. 266) lorsque des événements définis se produisent pendant l'utilisation du logiciel. Vous pouvez choisir le mode de notification pour chaque événement : courrier électronique, avertissement sonore, infobulle.

- Ajout de la technologie d'autodéfense du logiciel, de protection contre l'administration à distance et de protection de l'accès aux paramètres du logiciel grâce à l'instauration d'un mot de passe. Ceci permet d'éviter que des programmes malveillants, des personnes animées de mauvaises intentions ou des utilisateurs non qualifiés ne désactivent la protection.

- Utilisation d'une technologie de restauration du système qui permet de supprimer de la base de registres système et du système de fichiers de l'ordinateur le code malveillant et de rétablir le système à son état antérieur à l'attaque du code malveillant.

Nouveautés au niveau de l'interface

- La nouvelle interface de Kaspersky Internet Security offre un accès simple et convivial à n'importe quelle fonction de l'application. Vous pouvez également modifier l'apparence du logiciel en créant et en utilisant vos propres éléments graphiques et la palette de couleurs.

- Vous recevez toutes les informations relatives au fonctionnement de l'application : Kaspersky Internet Security émet des messages sur l'état de la protection, joint des commentaires et des conseils à ses actions et offre une rubrique d'aide détaillée.

Nouveautés au niveau de la mise à jour du programme

- Cette version du logiciel intègre une procédure de mise à jour améliorée : désormais, Kaspersky Internet Security surveille lui-même la publication des mises à jour des signatures des menaces et des modules de l'application indispensables à son fonctionnement. La mise à jour est réalisée automatiquement dès qu'il est possible d'établir une connexion avec un serveur de mise à jour de Kaspersky Lab.
- Seules les données qui vous manquent sont téléchargées. Cela permet de réduire par 10 le volume téléchargé lors de la mise à jour.
- Lors de la mise à jour, le système détermine la source de mise à jour la plus efficace et tentera de s'y connecter en premier à l'avenir.
- Il est désormais possible de ne pas utiliser un serveur proxy si la mise à jour du logiciel est réalisée au départ d'une source locale. Cela permet de réduire considérablement le volume du trafic qui transite via le serveur proxy.
- Possibilité de remettre les mises à jour à l'état initial, ce qui permet de récupérer une version exploitable des bases en cas de corruption des fichiers ou d'erreur de copie des mises à jour.

2.2. Configuration de la protection offerte par Kaspersky Internet Security

La protection offerte par Kaspersky Internet Security est configurée en fonction de la source de la menace. Autrement dit, un composant est prévu pour chaque source. Ce composant contrôle la source et prend les mesures qui s'imposent pour éviter toute action malveillante en provenance de cette source sur les données de l'utilisateur. 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 :

Des composants de protection (cf. point 2.2.1, p. 26) qui protège tous les canaux de transfert de données de et vers votre ordinateur.

Des tâches de recherche de virus (cf. point 2.2.2, p. 28) qui procède à la recherche d'éventuels virus dans l'ordinateur ou dans des fichiers, des répertoires, des disques ou des secteurs particuliers.

Des services (cf. point 2.2.3, p. 29) qui garantissent le soutien information dans le cadre de l'utilisation du logiciel et qui permettent d'en élargir les fonctions.

2.2.1. Composants de protection

La protection en temps réel de l'ordinateur est assurée par les composants suivants :

Antivirus Fichiers

Le système de fichiers peut contenir des virus et d'autres programmes dangereux. Les programmes malveillants peuvent rester des années dans le système de fichiers de votre ordinateur sans jamais se manifester. Il suffit cependant d'ouvrir le fichier infecté ou essayer de le copier sur le disque pour qu'il se réveille.

L'antivirus fichiers est le composant qui contrôle le système de fichiers de l'ordinateur. Il analyse tous les fichiers OUVERTS, EXECUTES et ENREGISTRES sur l'ordinateur et tous les disques connectés. Chaque fichier sollicité sera intercepté par Kaspersky Internet Security et soumis à une analyse antivirus pour trouver des virus connus. L'utilisation ultérieure du fichier sera possible uniquement si le fichier n'est pas infecté ou s'il a été bien réparé. Si le fichier ne peut pas être réparé pour une raison quelconque, il sera supprimé (dans ce cas, une copie du fichier est placée dans le dossier de sauvegarde) (cf. point 16.2, p. 235)ou mis en quarantaine (cf. point 16.1, p. 231).

Antivirus Courrier

Le courrier électronique est souvent utilisé par les personnes malveillantes pour diffuser les programmes malveillants. Il s'agit d'un des principaux vecteurs de diffusion des vers. Pour cette raison, il est capital de contrôler tous les messages électroniques.

L'*antivirus de courrier électronique* est le composant qui analyse tout le courrier entrant et sortant de l'ordinateur. Il recherche la présence éventuelle de programmes malicieux dans les messages électroniques. Le destinataire pourra accéder au message uniquement si ce dernier ne contient aucun objet dangereux.

Antivirus Internet

Lorsque vous ouvrez différents sites Internet, vous risquez d'infecter votre ordinateur avec les virus associés aux scripts exécutés sur le site ou de télécharger des objets dangereux.

L'antivirus Internet a été tout spécialement conçu pour éviter de telles situations. Ce composant intercepte le script du site et bloque son

exécution si le script constitue une menace. Tout le trafic http est également surveillé de près.

Défense proactive

Le nombre de programmes malveillants augmente chaque jour, ils deviennent plus sophistiqués, regroupes les propriétés de divers types et les méthodes de diffusion deviennent de plus en plus difficile à identifier.

Afin pouvoir identifier un nouveau programme malveillant avant qu'il n'ait pu causer des dégâts, Kaspersky Lab a mis au point un composant spécial : *la défense proactive*. Il repose sur le contrôle et l'analyse du comportement de tous les programmes installés. Sur la base des actions réalisées, Kaspersky Internet Security décide s'il s'agit d'un programme dangereux ou non. Ainsi, votre ordinateur est protégé non seulement contre les virus connus mais également contre ceux qui n'ont pas encore été étudiés.

Anti-Escroc

Les programmes qui affichent des publicités non sollicitées (fenêtres pop up, bannières), les programmes réalisant des connexions non-autorisées vers des sites Web payant, divers outils d'administration à distance et de surveillance, jokewares, etc. se sont fortement répandus au cours de ces derniers temps.

Anti-Escroc surveille ces actions et bloque leur exécution. Ainsi, le composant bloque les bannières et les fenêtres pop up qui gênent l'internaute dans ses activités, il bloque les programmes qui tentent d'établir une connexion non autorisée et analyse les pages Web afin de voir si elles sont associées à une attaque de phishing.

Anti-Hacker

Les pirates informatiques exploitent n'importe quelle "faille" pour pénétrer dans les ordinateurs, qu'il s'agisse d'une connexion ouverte à un réseau, du transfert d'informations d'ordinateur à ordinateur, etc.

Anti-Hacker est un composant qui a été conçu pour protéger votre ordinateur lorsque vous êtes connecté à Internet ou à tout autre réseau. Il surveille les connexions entrantes et sortantes et analyse les ports et les paquets de données.

Anti-Spam

Bien que le courrier indésirable ne représente pas une menace directe, il augmente la charge du serveur de messagerie, pollue la boîte de réception des utilisateurs et entraîne des pertes de temps, et par conséquences des pertes financières.

Le composant *Anti-Spam* s'intègre au client de messagerie installé sur votre ordinateur et vérifie tous les messages entrant afin de voir s'il s'agit de courrier non sollicité. Un titre spécial est ajouté à tous les messages indésirables. Il est possible également de configurer Anti-Spam pour le traitement du courrier indésirable (suppression automatique, placement dans un dossier spécial, etc.).

2.2.2. Tâches de recherche de virus

En plus de la protection en temps réel de tous les canaux par lesquels des programmes malveillants pourraient s'introduire sur votre ordinateur, il est important de procéder régulièrement à une analyse antivirus de l'ordinateur. Cette activité est indispensable afin d'éviter la propagation de programmes malveillants qui n'auraient pas été interceptés par les composants de la protection en raison d'un niveau de protection trop bas ou de tout autre motif.

Kaspersky Internet Security contient trois tâches axées sur la recherche des virus :

Secteurs critiques

Recherche d'éventuels virus dans tous les secteurs critiques de l'ordinateur. Il s'agit de la mémoire système, des objets utilisés au démarrage du système, des secteurs d'amorçage des disques et des répertoires système *Windows* et *system32*. L'objectif poursuivi est d'identifier rapidement les virus actifs dans le système sans devoir lancer une analyse complète de l'ordinateur.

Mon poste de travail

Recherche d'éventuels virus sur votre ordinateur avec analyse minutieuse de tous les disques connectés, de la mémoire et des fichiers.

Objets de démarrage

Recherche d'éventuels virus dans les objets chargés lors du démarrage du système d'exploitation, ainsi que la mémoire vive et les secteurs d'amorçage des disques.

Les experts de Kaspersky Lab recommande d'exécuter ces tâches au moins une fois par semaine.

Il est possible également de créer d'autres tâches de recherche de virus et de programmer leur lancement. Par exemple, il est possible de créer une tâche pour l'analyse des bases de messagerie une fois par semaine ou une tâche pour la recherche d'éventuels virus dans le répertoire **Mes documents**.

2.2.3. Services du programme

Kaspersky Internet Security propose divers services. Ceux-ci visent à maintenir le logiciel à jour, à élargir les possibilités d'utilisation du programme et à fournir de l'aide pendant l'utilisation du programme.

Mise à jour

Afin d'être toujours prêt à repousser n'importe quelle attaque de pirate, à neutraliser tout virus ou programme malveillant, à intercepter le courrier indésirable, il faut veiller à ce que Kaspersky Internet Security soit toujours à jour. Le composant *Mise à jour* a été conçu à cette fin. Il assure la mise à jour des signatures des menaces et des modules de Kaspersky Internet Security utilisés.

Rapport

Un rapport est généré pendant l'utilisation du programme pour chaque composant, chaque tâche de recherche de virus exécutée ou mise à jour. Ce rapport contient les informations relatives aux opérations exécutées et à leur résultats. Grâce à la fonction *Rapports*, vous pourrez toujours vérifier en détail le fonctionnement de n'importe quel composant de Kaspersky Internet Security. Si un problème survient, il est possible d'envoyer les rapports à Kaspersky Lab où ils seront étudiés en détails par nos spécialistes qui tenteront de vous aider le plus vite possible.

Kaspersky Internet Security déplacent tous les objets suspects du point de vue de la sécurité dans un répertoire spécial : la *quarantaine*. Ces objets sont cryptés, ce qui permet d'éviter l'infection de l'ordinateur. Ces objets pourront être soumis à une analyse antivirus, restaurés dans leur emplacement d'origine, supprimés ou ajoutés indépendamment dans la quarantaine. Tous les objets jugés sains après l'analyse sont automatiquement restaurés dans leur emplacement d'origine.

Le *dossier de sauvegarde* contient les copies des objets réparés ou supprimés par le programme. Ces copies sont créées au cas où il faudra absolument restaurer l'objet ou le scénario de son infection. Les copies de sauvegarde des objets sont également chiffrées afin d'éviter l'infection de l'ordinateur.

Il est possible de restaurer la copie de sauvegarde depuis ce dossier vers son emplacement d'origine ou de la supprimer.

Disque de secours

Kaspersky Internet Security propose un service spécial qui permet de créer un disque de secours pour restaurer le système.

La création d'un tel disque est utile lorsque les fichiers système ont été endommagés par une attaque de virus et qu'il est impossible de charger le système d'exploitation. Dans ce cas, grâce au disque de secours, vous pourrez démarrer l'ordinateur et restaurer le système à son état antérieur à l'infection.

Assistance technique

Tous les utilisateurs enregistrés de Kaspersky Internet Security ont accès au service d'assistance technique. Utilisez la fonction Assistance technique pour savoir où vous pouvez obtenir l'assistance technique dont vous avez besoin.

Vous pouvez consulter la liste des questions fréquemment posées afin de trouver la réponse à votre problème. Vous pouvez également accéder au service d'assistance technique en ligne. Consulter notre site . Consultez notre site http://support.kaspersky.fr/ pour en savoir plus.

2.3. Configurations matérielle et logicielle

Pour garantir le fonctionnement normal de Kaspersky Internet Security 6.0, l'ordinateur doit répondre aux conditions minimum suivantes :

Configuration générale :

- 50 Mo d'espace disque disponible.
- Lecteur de cédérom (pour installer Kaspersky Internet Security 6.0 à partir du cédérom).
- Microsoft Internet Explorer 5.5 ou suivant (pour la mise à jour des signatures des menaces et des modules de l'application via Internet).
- Microsoft Windows Installer 2.0.
- Liaison Internet active pour les mises à jour des bases antivirales.
- Processeur Intel Pentium 300 Mhz ou supérieur.
- 64 Mo de mémoire vive disponible.

Microsoft Windows 2000 Professional (Service Pack 2 ou suivant), Microsoft Windows XP Home Edition, Microsoft Windows XP Professional (Service Pack 1 ou suivant):

- Processeur Intel Pentium 300 Mhz ou supérieur.
- 128 Mo de mémoire vive disponible.

2.4. Contenu du pack logiciel

Vous pouvez acquérir Kaspersky Internet Security® 6.0 chez un distributeur ou détaillant, ou visiter l'un de nos magasins en ligne (par exemple, http://www.kaspersky.com/fr – rubrique **Boutique en ligne / Particuliers**).

Le pack logiciel en boite contient :

- Le CD ROM d'installation où les fichiers du logiciel sont enregistrés
- Selon le mode d'achat de votre logiciel (téléchargement ou boîte), la licence d'utilisation pour la durée acquise peut se trouver :
    - sous la forme d'un code d'activation de 33 caractères (exemple de format xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx) imprimé sur le manuel d'utilisation ou la pochette du CD-Rom
    - sur le CDROM dans un fichier appelé clé de licence (xxxxxxx.key),
    - dans le programme d'installation lui-même,
- Le manuel de l'utilisateur avec le contrat de licence utilisateur imprimé à la fin de ce manuel.

Si vous achetez Kaspersky Anti-Virus® 6.0 en ligne, et dés la réception de votre paiement, vous recevrez un email contenant des liens personnels pointants sur La boutique en ligne de Kaspersky Lab pour télécharger :

- le fichier d'installation,
- la licence d'utilisation pour la durée acquise ,
- la version électronique du manuel (format Adobe PDF).

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

CHAPITRE 3. INSTALLATION DE KASPERSKY INTERNET SECURITY 6.0

Kaspersky Internet Security peut être installé partiellement ou complètement.

En cas d'installation partielle, vous pouvez sélectionner les composants à installer ou sélectionner l'installation automatique des seuls composants de la protection antivirus (cf. Etape 9 de la procédure d'installation). Libre à vous d'installer par la suite les autres composants, mais vous devrez pour ce faire utiliser le fichier d'installation original. Pour cette raison, il est conseillé de copier le fichier de l'installation du logiciel sur le disque dur ou de lancer l'installation au départ de la ligne de commande :

```
msiexec /a <fichier_d'installation>
```

Dans ce cas, Microsoft Windows Installer copiera automatiquement le fichier d'installation sur votre ordinateur.

3.1. Procédure d'installation

Afin d'installer Kaspersky Internet Security sur votre ordinateur, vous devez exécuter le fichier d'installation (fichier msi) repris sur le CD-ROM d'installation.

> Remarque.
>
> L'installation au départ d'un fichier téléchargé est en tout point identique à l'installation au départ du cédérom.

Le programme d'installation se présente sous la forme d'un Assistant. Chacune de ces boîtes présente différents boutons destinés à contrôler la procédure. En voici une brève description :

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

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

Etape 1. Vérification de l'existence des conditions minimales requises pour l'installation de Kaspersky Internet Security

Avant de procéder à l'installation du logiciel sur votre ordinateur, le système vérifie si le système d'exploitation et les services packs installés suffisent pour Kaspersky Internet Security. Le système vérifie également si les programmes requis sont présents et si vous jouissez des privilèges suffisants pour installer l'application.

Un message vous préviendra si une des conditions n'est pas remplie. Il est conseillé d'installer les mises à jour requises à l'aide de **Windows Update** ainsi que les autres programmes nécessaires avant d'installer Kaspersky Internet Security.

Etape 2. Fenêtre d'accueil de la procédure d'installation

Si votre système répond aux conditions d'installation, la fenêtre de bienvenue s'affichera dès le lancement du fichier d'installation. Elle contient des renseignements sur le début de l'installation de Kaspersky Internet Security.

Cliquez sur **Suivant** pour poursuivre l'installation Cliquez sur **Annuler** pour interrompre l'installation.

Etape 3. Examen du contrat de licence

Cette fenêtre reprend le contrat de licence entre l'utilisateur et Kaspersky Lab. Lisez-le attentivement est si vous acceptez les dispositions, sélectionnez l'option **J'accepte le contrat de licence** puis, cliquez sur **Suivant**. L'installation passera à l'étape suivante.

Etape 4. Sélection du dossier d'installation

Cette étape vous permet de sélectionner le répertoire dans lequel vous souhaitez installer Kaspersky Internet Security. Il s'agit par défaut de : **<Disque>\Program Files\Kaspersky Lab\Kaspersky Internet Security 6.0**.

Vous pouvez sélectionner un autre répertoire à l'aide du bouton **Parcourir** qui ouvre la boîte de dialogue standard de sélection de répertoire ou en saisissant le chemin d'accès au répertoire dans le champ prévu à cet effet.

Si vous saisissez le nom du répertoire manuellement, sachez qu'il ne peut pas contenir plus de 200 caractères, ni des caractères spéciaux.

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

Etape 5.Choix du type d'installation

Vous devez décider à ce stade du type d'installation. Trois options s'offrent à vous :

Complète. Tous les composants de Kaspersky Internet Security seront installés sur votre ordinateur. Pour voir la suite de l'installation, consultez l'Etape 7.

Personnalisée. Dans ce cas, vous pouvez sélectionner les composants que vous souhaitez installer. Pour de plus amples informations, consultez l'Etape 6

Composants de la protection antivirus. Cette option vous permet d'installer uniquement les composants chargés de la protection antivirus de votre ordinateur. Anti-Hacker, Anti-Spam et Anti-Escroc ne seront pas installés.

Cliquez sur le bouton qui correspond au type d'installation souhaité.

Etape 6.Sélection des composants à installer

Cette étape vous concerne uniquement si vous avez sélectionné l'option **Personnalisée** pour l'installation du logiciel.

Lorsque vous décidez de réaliser une installation personnalisée, vous devez composer la liste des composants de Kaspersky Internet Security que vous souhaitez installer. Par défaut, les composants de la protection antivirus et le composant de recherche de virus sont sélectionnés. Anti-Hacker, Anti-Spam et Anti-Escroc ne seront pas installés.

Pour sélectionner un composant à installer, il faut ouvrir le menu contextuel d'un clic droit de la souris sur l'icône située à côté du nom du composant et sélectionner le point **Le composant sera installé sur le disque dur local**. La partie inférieure de cette fenêtre du programme d'installation vous fournira de plus amples informations sur le type de protection assurée par le composant sélectionné et l'espace disque requis.

Si vous ne souhaitez pas installer un composant, sélectionnez le point **Le composant ne sera pas accessible** dans le menu contextuel. N'oubliez pas qu'en décidant de ne pas installer tel ou tel composant, vous vous exposez à toute une série de programmes dangereux.

Une fois que vous aurez opéré votre sélection, cliquez sur **Suivant**. Pour revenir à la liste des composants à installer, cliquez sur **Annuler**.

Etape 7. Désactivation du pare-feu de Microsoft Windows

Cette étape se présente uniquement si Kaspersky Internet Security est installé sur un ordinateur qui possède un pare-feu actif et que Anti-Hacker figure parmi les composants qui seront installés.

Cette étape de l'installation de Kaspersky Internet Security vous propose de désactiver le pare-feu de Microsoft Windows car le composant Anti-Hacker, qui fait partie de Kaspersky Internet Security, vous protège complètement lorsque vous êtes connecté au réseau et que dès lors, il n'est pas nécessaire d'utiliser les moyens de protection offerts par le système d'exploitation.

Si vous souhaitez utiliser Anti-Hacker en guise de pare-feu, cliquez sur **Suivant**. Le pare-feu de Microsoft Windows sera désactivé automatiquement.

Si vous souhaitez protéger votre ordinateur à l'aide du pare-feu de Microsoft Windows, sélectionnez l'option **Utiliser le pare-feu de Microsoft Windows**. Dans ce cas, Anti-Hacker sera installé mais sera désactivé pour éviter tout conflit.

Etape 8. Recherche des programmes pouvant nuire à la bonne installation

Au cours de cette étape, tous les programmes chargés sur l'ordinateur sont analysés. L'écran affichera le nom de tout programme qui pourrait nuire à la bonne installation de Kaspersky Internet Security. Vous devrez arrêter ces programmes avant de poursuivre l'installation.

Il peut s'agir par exemple de Microsoft Office Outlook. S'il est ouvert au moment de l'installation de Kaspersky Internet Security, il est possible qu'Anti-Spam ne soit pas installé correctement. Lors de l'installation de ce composant, un plug in est intégré à Microsoft Office Outlook afin d'entraîner Anti-Spam sur la base des messages que vous recevez et d'affiner ainsi l'identification et le traitement du courrier indésirable.

Une fois que vous aurez quitté le programme, cliquez sur **Suivant** afin de poursuivre l'installation.

Etape 9. Recherche d'autres logiciels antivirus éventuellement installés

Cette étape correspond à la recherche d'autres logiciels antivirus installés, y compris d'autres logiciels de Kaspersky Lab, dont l'utilisation conjointe à celle de Kaspersky Internet Security pourrait entraîner des conflits.

Si de tels programmes existent sur votre ordinateur, leur nom apparaîtra à l'écran. Vous pourrez les supprimer avant de poursuivre l'installation.

En-dessus de la liste des logiciels antivirus découverts, vous pourrez décider de les supprimer automatiquement ou manuellement.

Si Kaspersky Anti-Virus Personal ou Kaspersky Anti-Virus Personal Pro figurent parmi cette liste, il est conseillé de conserver les clés de licence utilisées par ces logiciels avant de les supprimer. Vous pourrez en effet les utiliser en tant que clé pour Kaspersky Internet Security 6.0. Il est conseillé également de conserver les objets de la quarantaine et du dossier de sauvegarde. Ces objets seront placés automatiquement dans les répertoires correspondant de Kaspersky Internet Security et vous pourrez continuer à les manipuler.

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

Etape 10. Préparation finale pour l'installation de l'application

Cette étape constitue la préparation finale pour l'installation du logiciel sur votre ordinateur. Vous pouvez décider d'utiliser les paramètres de protection, les signatures des menaces et la base des connaissances d'Anti-Spam si ceux-ci ont été enregistrés sur l'ordinateur lors de la suppression de la version antérieure de Kaspersky Internet Security (par exemple, vous aviez installé la version bêta et vous installez maintenant la version commerciale).

Voyons comment utiliser les possibilités décrites ci-dessus.

Si une version antérieure de Kaspersky Internet Security était déjà installée sur votre ordinateur et que, au moment de la supprimer, vous avez conservé les signatures des menaces, vous pourrez les utiliser avec la version que vous installer. Pour ce faire, cochez la case ☑ **Signatures des menaces.** Les signatures des menaces livrées avec le programme ne seront dès lors pas copiées sur votre ordinateur.

Pour utiliser les paramètres de protection définis dans la version antérieure que vous aviez sauvegardés, cochez la case ☑ **Paramètres de protection**.

Il est conseillé également d'utiliser la base de connaissance d'Anti-Spam si vous l'aviez sauvegardée lors de la suppression de la version antérieure du programme. Vous ne devrez pas ainsi entraîner à nouveau Anti-Spam. Pour tenir compte de la base des connaissances que vous aviez créée, cochez la case ☑ **Base de connaissances d'Anti-Spam**.

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

Etape 11. Lecture des informations importantes relatives à l'application

Cette fenêtre vous donne la possibilité de prendre connaissance de renseignements importants sur le logiciel avant de commencer à l'utiliser. Vous y trouverez une brève description des principales caractéristiques de Kaspersky Internet Security, les particularités de son fonctionnement, etc., les particularités de son fonctionnement, etc.

Pour passer à l'étape suivante de l'installation, cliquez sur **Suivant**.

Etape 12. Fin de la procédure d'installation

La fenêtre **Fin de l'installation** reprend des informations relatives à la fin de l'installation de Kaspersky Internet Security sur votre ordinateur.

Si le redémarrage de l'ordinateur s'impose pour finaliser l'installation, le message correspondant s'affichera. Après le redémarrage, l'Assistant de configuration initiale de Kaspersky Internet Security sera lancé automatiquement.

Si le redémarrage de l'application n'est pas nécessaire pour finaliser l'installation, cliquez sur Suivant afin de passer à l'Assistant de configuration initiale du logiciel.

3.2. Assistant de configuration initiale

L'Assistant de configuration de Kaspersky Internet Security 2006 est lancé à la fin de la procédure d'installation du logiciel. Son rôle est de vous aider à réaliser la configuration initiale du logiciel sur la base des particularités et des tâches de votre ordinateur.

L'interface de l'Assistant de configuration se présente sous la forme d'un Assistant Windows composé d'une succession de fenêtres (étapes). La navigation entre ces fenêtres s'effectue via les boutons **Précédent** et **Suivant**. Pour quitter l'Assistant, cliquez sur **Terminer**. Pour arrêter l'Assistant à n'importe quel stade, cliquez sur **Annuler**.

Vous pouvez ignorer la configuration initiale lors de l'installation du programme en fermant l'Assistant. Vous pourrez lancer ultérieurement l'Assistant au départ de l'interface du logiciel en rétablissant les paramètres d'origine de Kaspersky Internet Security (cf. point 6.7, p. 88).

3.2.1. Utilisation des objets sauvegardés de la version 5.0

Cette fenêtre de l'Assistant s'affiche si la version 5.0 de Kaspersky Anti-Virus était installée et que des objets de la quarantaine ou du dossier de sauvegarde, les données d'activation (clé de licence) ou les paramètres de protection ont été préservés lors de la suppression de cette version.

Pour utiliser ces objets avec la version 6.0, cochez les cases adéquates

3.2.2. Activation du logiciel

La procédure d'activation du logiciel consiste à installer la licence que Kaspersky Internet Security utilisera pour confirmer la présence d'un contrat de licence et sa durée de validité.

La clé de licence contient les informations de service indispensables pour assurer le parfait fonctionnement du logiciel ainsi que des renseignements complémentaires :

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

Attention !

Activer le logiciel maintenant (requiert l'accès à Internet) Si vous n'êtes pas connecté à Internet au moment de l'installation, vous pouvez réaliser l'activation plus tard au départ de l'interface du logiciel (cf. point **Error! Reference source not found.**, p. **Error! Bookmark not defined.**).

3.2.2.1. Sélection du mode d'activation du programme

L'activation du logiciel se fait de différentes façons selon votre cas :

- **Activer à l'aide du code d'activation**. Sélectionnez cette option si vous êtes en possession d'un code d'activation. Sur la base de ce code, la licence commerciale s'activera automatiquement pour toute sa durée de validité.
- **Activer la version d'évaluation (30 jours)**. Sélectionnez cette option si vous souhaitez installer une version d'évaluation du logiciel avant de décider d'acheter la version commerciale. La licence sera valide 30 jours non-renouvelable.

- **Utiliser votre clé de licence acquise antérieurement non expirée**. Sélectionnez cette option si vous possédez déjà une clé de licence valide pour ce logiciel Kaspersky .
- **Activer le logiciel plus tard**. Sélectionnez cette option si vous êtes en attente de votre licence commerciale. L'activation du logiciel sera reportée à plus tard. Ce logiciel Kaspersky sera installé sur l'ordinateur et vous aurez accès à toutes les fonctions, à l'exception de la mise à jour (vous pourrez actualiser les signatures des menaces une fois que vous aurez activé le logiciel au moyen d'un des trois points précédents).

3.2.2.2. Saisie du code d'activation

Saisissez le code d'activation que vous avez reçu à l'achat du logiciel.

Saisissez vos coordonnées dans la fenêtre d'activation : nom, prénom, courrier électronique, pays et ville. Ces informations servent à identifier les utilisateurs enregistrés, par exemple en cas de dégradation ou de vol de la licence. Dans ce cas, vous pourrez obtenir une copie de votre licence sur la base des coordonnées que vous aurez fournies.

3.2.2.3. Principe d'activation de la licence par le code d'activation

L'Assistant de configuration établit une connexion via Internet avec les serveurs de Kaspersky Lab et envoie vos données d'enregistrement (code d'activation, coordonnées) qui seront vérifiées sur ces serveurs.

Si le code d'activation est correct, le logiciel s'activera automatiquement pour la durée de la licence

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

3.2.2.4. Principe d'activation de la licence par le fichier de licence

Si vous possédez un fichier de clé de licence valide pour ce logiciel , cette boîte de dialogue vous invitera à l'installer. Pour ce faire, cliquez sur **Parcourir** et dans la boîte de dialogue standard de sélection des fichiers, sélectionnez le fichier de clé (format du nom de fichier : xxxxxxx.*key*).

Une fois la clé installée, les informations relatives à la licence seront reprises dans la partie inférieure de la fenêtre : nom du détenteur, numéro de licence, type (commerciale, test bêta, évaluation, etc.) et fin de validité de la licence.

3.2.2.5. Fin de l'activation du logiciel

L'Assistant de configuration vous informe de la réussite de l'activation du logiciel. Il fournit également des renseignements relatifs à la licence installée : nom du détenteur, numéro de licence, type (commerciale, évaluation, etc.) et date de fin de validité de la licence.

3.2.3. Configuration de la mise à jour

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

- **Automatique**. Dans ce cas, Kaspersky Internet Security lance la copie et l'installation de mises à jour au fur et à mesure qu'elles sont publiées sur le serveur. Ce mode est activé par défaut.
- **Tous les jours à 15h30** (l'intervalle peut varier en fonction des paramètres de programmation). La mise à jour sera lancée automatiquement selon l'horaire défini. Les paramètres de la programmation peuvent être définis dans la boîte de dialogue qui s'ouvre après avoir cliqué sur **Modifier**.
- **Manuel**. Vous lancez vous-même la procédure de mise à jour du logiciel.

N'oubliez pas que les bases des signatures des menaces et les modules du logiciel qui font partie de l'installation peuvent être dépassés au moment de l'installation. Pour cette raison, nous vous conseillons d'obtenir les mises à jour les plus récentes du logiciel. Il suffit simplement de cliquer sur **Mettre à jour**. Dans ce cas, Kaspersky Internet Security recevra toutes les mises à jour depuis Internet et les installera sur l'ordinateur.

Si vous souhaitez passer à la configuration des mises à jour (sélectionner les paramètres de réseau, sélectionner la ressource au départ de laquelle la mise à jour sera réalisée, indiquer le serveur de mise à jour le plus proche de votre emplacement), cliquez sur **Configuration**.

3.2.4. Programmation de la recherche de virus

La recherche des objets malveillants dans certains secteurs est l'une des tâches les plus importantes pour la protection de votre ordinateur.

Lors de l'installation de Kaspersky Internet Security, trois tâches d'analyse sont créées par défaut. Cette fenêtre de l'Assistant de configuration vous permet de sélectionner le mode de lancement de la tâche d'analyse :

Analyse des objets de démarrage

- **Après l'allumage de l'ordinateur** : analyse automatiquement les objets de démarrage chaque fois que l'ordinateur est allumé. Ce mode d'analyse est activé par défaut.
- **Après chaque mise à jour** : analyse automatiquement les objets de démarrage après le téléchargement des dernières mises à jour.

Vous pouvez activer le lancement automatique de l'analyse des objets de démarrage dans les deux cas. Pour ce faire, cochez les cases correspondantes.

Analyse des secteurs critiques

Pour lancer automatiquement l'analyse des secteurs critique de l'ordinateur (mémoire système, objets de démarrage, secteurs d'amorçage, répertoires système Microsoft Windows), cochez la case dans le bloc correspondant. Les paramètres de la programmation peuvent être définis dans la boîte de dialogue qui s'ouvre après avoir cliqué sur **Modifier**.

Le lancement automatique de cette tâche est désactivé par défaut.

Analyse complète de l'ordinateur

Pour lancer automatiquement l'analyse complète de l'ordinateur, cochez la case dans le bloc correspondant. Les paramètres de la programmation peuvent être définis dans la boîte de dialogue qui s'ouvre après avoir cliqué sur **Modifier**.

Le lancement programmé de cette tâche est désactivé par défaut. Nous vous conseillons toutefois de lancer l'analyse complète de l'ordinateur directement après l'installation du logiciel.

3.2.5. Restriction de l'accès au logiciel

Dans la mesure où votre ordinateur peut être utilisé par différentes personnes (par exemple, les membres de votre famille) et que leurs connaissances informatiques peuvent être faibles et vu que certains programmes malveillants peuvent désactiver la protection, vous avez la possibilité de définir un mot de passe pour limiter l'accès à Kaspersky Internet Security. Le mot de passe protège le logiciel contre les tentatives de désactivation non autorisée ou de modification des paramètres de la protection.

Afin d'activer cette option, cochez la case **Activer la protection par mot de passe** et saisissez les informations dans les champs **Mot de passe** et **Confirmation du mot de passe**.

Indiquez ensuite les tâches qui seront concernées :

- **Toutes les opérations du logiciel (à l'exception de la découverte d'objets dangereux).** Le mot de passe est nécessaire pour lancer n'importe quelle action du logiciel à l'exception de la manipulation des messages relatifs à la découverte d'objets dangereux.
- **Sélectionnez les actions protégées par un mot de passe:**
  - **Enregistrement des paramètres de fonctionnement du logiciel** : le mot de passe est requis lorsque l'utilisateur tente d'enregistrer les modifications apportées aux paramètres du logiciel.
  - **Quitter le logiciel** : le mot de passe est requis pour quitter le logiciel.
  - **Arrêt/pause des composants de la protection et des tâches de recherche de virus** : le mot de passe est requis pour suspendre ou arrêter n'importe quel composant ou n'importe quelle tâche liée à la recherche de virus.

3.2.6. Configuration des paramètres d'Anti-Hacker

Anti-Hacker est un composant de Kaspersky Internet Security qui garantit la sécurité de votre ordinateur sur Internet et dans les réseaux locaux. L'Assistant de configuration vous propose à cette étape de rédiger une série de règles qui seront suivies par Anti-Hacker pour l'analyse de l'activité de réseau de votre ordinateur.

3.2.6.1. Définition du statut de la zone de protection

Cette étape de la configuration à l'aide de l'Assistant correspond à l'analyse de l'environnement de réseau de votre ordinateur. Sur la base des résultats de l'analyse, le réseau est scindé en zones conventionnelles :

Internet, le réseau des réseaux. Dans cette zone, Kaspersky Internet Security fonctionne comme un pare-feu personnel. Toute l'activité de réseau est régie par les règles pour les paquets et les applications créées par défaut afin d'offrir une protection maximale. Vous ne pouvez pas modifier les conditions de la protection lorsque vous évoluez dans cette zone, si ce n'est activer le mode furtif de l'ordinateur afin de renforcer la protection.

Zones de sécurité, quelques zones conventionnelles qui correspondent souvent aux sous-réseaux auxquels votre ordinateur est connecté (il peut s'agir d'un sous-réseau local à la maison ou au bureau). Par défaut, ces zones sont considérées comme des zones à risque moyen. Vous pouvez modifier le statut de ces zones sur la base de la confiance accordée à un sous-réseau ou l'autre et configurer des règles pour les paquets et les applications.

Toutes les zones identifiées sont reprises dans une liste. Elles sont toutes accompagnées d'une description, de l'adresse et du masque de sous-réseau ainsi que de l'état qui déterminera l'autorisation ou non d'une activité de réseau quelconque dans le cadre du fonctionnement d'Anti-Hacker :

- **Internet**. Cet état est attribué par défaut au réseau Internet car une fois qu'il y est connecté, l'ordinateur est exposé à tout type de menaces. Il est également conseillé de choisir cet état pour les réseaux qui ne sont protégés par aucun logiciel antivirus, pare-feu, filtre, etc. Cet état garantit la protection maximale de l'ordinateur dans cette zone, à savoir :

    - Le blocage de n'importe quelle activité de réseau NetBios dans le sous-réseau;
    - L'interdiction de l'exécution des règles pour les applications et les paquets qui autorisent l'activité de réseau NetBios dans le cadre de ce sous-réseau.

    Même si vous avez créé un dossier partagé, les informations qu'il contient ne seront pas accessibles aux utilisateurs d'un sous-réseau de ce type. De plus, lors de la sélection de cet état de réseau, vous ne pourrez pas accéder aux fichiers et aux imprimantes des autres ordinateurs du réseau.

- **Réseau local**. Cet état est attribué par défaut à la majorité des zones de sécurité découvertes lors de l'analyse de l'environnement de réseau de l'ordinateur, à l'exception d'Internet. Il est conseillé de choisir cet état pour les zones qui représentent un risque moyen (par exemple, le réseau Interne d'une entreprise). En choisissant cet état, vous autorisez :
    - Toute activité de réseau NetBios dans le cadre du sous-réseau.
    - L'exécution des règles pour les applications et les paquets qui autorisent l'activité de réseau NetBios dans le cadre du sous-réseau donné.

  Sélectionnez cet état si vous souhaitez autoriser l'accès à certains répertoires de votre ordinateur et interdire toute autre activité externe. Les utilisateurs auront ainsi accès aux répertoires partagés, mais ils ne pourront pas exécuter un cheval de Troie.
- **Réseau de confiance**. Cet état doit être réservé uniquement aux zones qui, d'après vous, ne présentent aucun danger, c.-à-d. les zones où l'ordinateur ne sera pas exposé à des attaques ou à des tentatives d'accès non autorisé. Le choix de cet état implique l'autorisation de n'importe quelle activité de réseau. Même si vous avez sélectionné le niveau de protection maximale et que vous avez créé des règles d'interdiction, ces paramètres ne seront pas applicables aux ordinateurs distants de la zone de confiance.

Pour les réseaux dont l'état est **Réseau local** ou **Internet**, vous pouvez activer le *mode furtif* pour plus de sécurité. Ce mode autorise uniquement l'activité initialisée par l'utilisateur ou une application autorisée. En d'autres termes, votre ordinateur devient "invisible" pour le monde extérieur. Vous pouvez toutefois continuer à utiliser Internet sans aucune difficulté.

Il n'est pas conseillé d'utiliser le mode furtif si l'ordinateur est utilisé en tant que serveur (ex. : serveur de messagerie ou serveur http). Si tel est le cas, les ordinateurs qui essaient de contacter ce serveur ne le verront pas dans le réseau.

Pour modifier l'état d'une zone ou pour activer/désactiver le mode furtif, sélectionnez l'état dans la liste et cliquez sur les liens requis dans le bloc **Description** situé sous la liste. Vous pouvez réaliser les mêmes actions ainsi que modifier l'adresse et le masque du sous réseau dans la fenêtre **Paramètres de la zone** ouverte à l'aide du bouton **Modifier**.

Lors de la consultation de la liste des zones, vous pouvez en ajouter un nouveau, à l'aide du bouton **Chercher**. Anti-Hacker recherchera les réseaux enregistrables et, s'il en trouve, il vous propose d'en définir l'état. De plus, il est possible d'ajouter une nouvelle zone à la liste manuellement (par exemple, si vous raccordez votre ordinateur portable à un nouveau réseau). Pour ce faire,

cliquez sur **Ajouter** et saisissez les informations requises dans la fenêtre **Paramètres de la zone**.

Afin de supprimer un réseau de la liste, cliquez sur **Supprimer**.

3.2.6.2. Constitution de la liste des applications de réseau

L'Assistant de configuration analyse les logiciels installés sur l'ordinateur et constitue une liste des applications utilisées lors du travail en réseau.

Pour chacune de ces applications, Anti-Hacker crée une règle qui régit l'activité de réseau. Les règles sont créés sur la base des modèles des applications connues utilisées dans le réseau composés par Kaspersky Lab et livrés avec le logiciel.

La liste des application de réseau et les règles qui les gouvernent figurent dans la fenêtre de configuration de Anti-Hacker qui apparaît lorsque vous cliquez sur **Liste**.

En guise de protection complémentaire, vous pouvez désactiver la mise en cache des noms de domaine lors de l'utilisation d'Internet. Ce service réduit considérablement la durée de chargement des sites souvent visités mais il représente également une vulnérabilité dangereuse via laquelle les individus mal intentionnés peuvent organiser le vol de données en contournant le pare-feu. Ainsi, afin de renforcer la sécurité de votre ordinateur, il est conseillé de désactiver la conservation des données sur les noms de domaine dans la mémoire cache (cette option est sélectionnée par défaut).

3.2.7. Sélection du mode de protection

Cette fenêtre de l'Assistant de configuration vous permet de sélectionner le mode de protection du logiciel :

Elémentaire. Ce mode est sélectionné par défaut et convient à la majorité des utilisateurs qui n'ont pas une connaissance poussée des ordinateurs et des logiciels antivirus. Il prévoit le fonctionnement des différents composants selon le niveau de protection recommandé et informe les utilisateurs uniquement des événements dangereux (par exemple, la découverte d'un objet malveillant, l'exécution d'actions dangereuses).

Interactif. Ce mode offre une protection plus étendue par rapport à la protection élémentaire. Il permet de suivre les tentatives de modification des paramètres système, les activités suspectes ainsi que les activités non autorisées dans le réseau. Toutes ces actions peuvent être la manifestation d'un programme malveillant ou être tout à fait normales dans le cadre de

l'utilisation de l'ordinateur. Pour chaque cas individuel, vous devrez décider d'autoriser ou non l'action..
En cas de sélection de ce mode, précisez quand le mode interactif devra être utilisé :

- **Activer l'apprentissage d'Anti-Hacker** : affiche la demande de confirmation de l'utilisateur lorsque des applications installées établissent des connexions avec certaines ressources du réseau. Vous pouvez autoriser ou non ces connexions et configurer les règles de fonctionnement d'Anti-Hacker pour cette application. Lorsque le mode d'apprentissage est désactivé, Anti-Hacker fonctionne en mode de protection minimale : toutes les applications ont accès aux ressources du réseau.
- **Activer le monitorage de la base de registres système** : affiche la demande de confirmation de l'utilisateur lors de tentatives de modification de la base de registres système.
- **Activer la défense proactive étendue** : active l'analyse de toutes les activités suspectes des applications du système, y compris le lancement du navigateur avec les paramètres de la ligne de commande, l'intrusion dans les processus du programme et l'intrusion des intercepteurs de fenêtres (ces paramètres sont désactivés par défaut).

3.2.8. Fin de l'Assistant de configuration

La dernière fenêtre de l'Assistant vous propose de redémarrer l'ordinateur afin de finaliser l'installation de l'application. Ce redémarrage est indispensable à l'enregistrement correct des pilotes de certains composants de Kaspersky Internet Security.

Vous pouvez reporter le redémarrage de l'application, mais dans ce cas, certains composants de la protection ne fonctionneront pas.

CHAPITRE 4. INTERFACE DU LOGICIEL

L'interface de Kaspersky Internet Security est à la fois simple et conviviale. Ce chapitre est consacré à ses principaux éléments, à savoir :

- L'icône de la barre des tâches (cf. point 4.1, p. 47);
- Le menu contextuel (cf. point 4.2, p. 48);
- La fenêtre principale (cf. point 4.3, p. 49);
- Fenêtre de configuration du logiciel (cf. point 4.4, p. 52).

En plus de l'interface principale du logiciel, il existe des plug-in intégrés :

- Microsoft Office Outlook:recherche de virus (cf. point 8.2.2, p. 106) et recherche du courrier indésirable (cf. point 13.3.9, p. 198).,
- Microsoft Outlook Express (cf. point 13.3.10, p. 202).
- TheBat! (recherche de virus (cf. point 8.2.3, p. 108) et recherche du courrier indésirable (cf. point 13.3.11, p. 203).
- Microsoft Internet Explorer (cf. Chapitre 11, p. 141).
- Microsoft Windows Explorer (cf. point 14.2, p. 206).

Ceux-ci élargissent les possibilité des programmes cités car ils permettent d'administrer et de configurer les composants correspondants de Kaspersky Internet Security directement depuis leur interface respective.

4.1. Icône de la barre des tâches

L'icône de Kaspersky Internet Security apparaît dans la barre des tâches directement après son installation.

Cette icône est un indicateur du fonctionnement de Kaspersky Internet Security. 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 activée. Si l'icône n'est pas activée  (noir et blanc) cela signifie que la protection est désactivée ou que certains des composants de la protection sont désactivés (cf. point 2.2.1, p. 26).

L'icône de Kaspersky Internet Security change en fonction de l'opération exécutée :

 L'analyse d'un message électronique est en cours.

 L'analyse d'un script est en cours.

 L'analyse d'un fichier ouvert, enregistré ou exécuté par vous ou un programme quelconque est en cours.

 La mise à jour des signatures des menaces et des modules logiciels de Kaspersky Internet Security est en cours.

L'icône donne également accès aux éléments principaux de l'interface du logiciel : le menu contextuel (cf. point 4.2, p. 48) et la fenêtre principale (cf. point 4.3, p. 49);

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

Pour ouvrir la fenêtre principale de Kaspersky Internet Security à l'onglet Protection (c'est l'onglet de départ proposé par défaut), double-cliquez avec le bouton gauche de la souris sur l'icône du programme. Si vous cliquez une seule fois, vous ouvrirez la fenêtre principale à la rubrique active lorsque vous avez quitté le programme la dernière fois.

4.2. Menu contextuel

Le menu contextuel (cf. ill. 1) permet d'exécuter toutes les tâches principales liées à la protection.

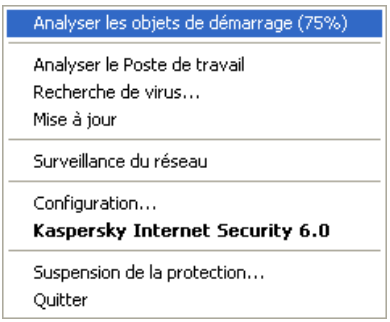


Illustration 1. Menu contextuel

Le menu de Kaspersky Internet Security contient les éléments suivants :

Analyser le poste de travail : 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. Par défaut, la liste comprend toute une série d'objets comme le dossier **Mes documents**, les objets de démarrage, les bases de messagerie, tous les disques de l'ordinateur, etc. Vous pouvez également compléter la liste, sélectionner des objets à analyser et lancer la recherche d'éventuels virus.

Mise à jour : télécharge les mises à jour des modules de l'application et des signatures de menaces de Kaspersky Internet Security et les installe sur l'ordinateur.

Surveillance du réseau : consultation de la liste des connexions établies, des ports ouverts et du trafic.

Activation : passe à l'activation du logiciel. Ce point apparaît uniquement si le programme n'est pas activé.

Configuration : permet d'examiner et de configurer les paramètres de fonctionnement de Kaspersky Internet Security.

Kaspersky Internet Security 6.0: ouvre la fenêtre principale de l'application (cf. point 4.3, p. 49).

Suspension de la protection/Activation de la protection : désactive temporairement/active le fonctionnement des composants de la protection (cf. point 2.2.1, p. 26). 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.

Quitter : quitte Kaspersky Internet Security.

Si une tâche quelconque de recherche de virus est lancée à ce moment, son nom apparaît dans le menu contextuel accompagné de la progression en pour cent. Après avoir sélectionné une tâche, vous pouvez consulter le rapport avec le résultat détaillé de l'exécution.

4.3. Fenêtre principale du logiciel

La fenêtre principale (cf. ill. 2) de Kaspersky Internet Security est constituée de deux panneaux :

- Le panneau de gauche est réservé à la *navigation*. Il permet de passer rapidement et simplement à n'importe quel composant, de lancer les recherches de virus et d'accéder aux services du logiciel;

- Le panneau de droite est à caractère *informatif* : il contient les informations relatives au composant sélectionné dans le panneau de gauche, permet d'accéder à la configuration de chacun d'entre eux, propose les instruments pour l'exécution de la recherche des virus, la manipulation des fichiers en quarantaine et des copies de réserve, la gestion des clés de licence, etc.

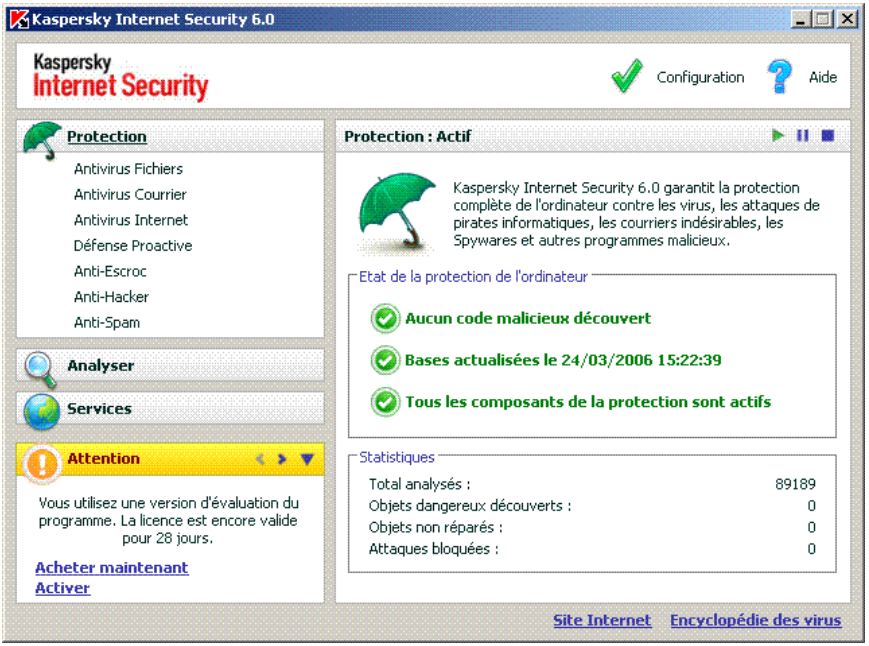
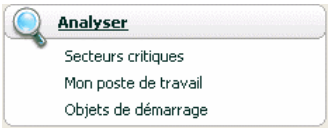


Illustration 2. Fenêtre principale de Kaspersky Internet Security

Dès que vous avez sélectionné une section ou un composant dans le panneau de gauche, le panneau de droite reprendra toutes les informations relatives au composant .

Examinons en détails les éléments du panneau de navigation de la fenêtre principale.

Section du panneau de navigation de la fenêtre principale	**Fonction**
La tâche principale de cette fenêtre est de vous informer sur l'état de la protection de votre ordinateur. La section **Protection** est prévue précisément à cette fin. 	Pour consulter les informations générales sur le fonctionnement de Kaspersky Internet Security, les statistiques de fonctionnement du logiciel, vérifier le bon fonctionnement de tous les composants, sélectionnez la section **Protection** dans le panneau de navigation. Pour consulter les paramètres d'un composant concret d'un composant, il suffit de sélectionner le nom du composant au sujet duquel vous souhaitez obtenir des informations dans la section **Protection**.
La section **Recherche de virus** est prévue pour la recherche d'objets malveillants. 	Cette section contient la liste des objets que vous pouvez soumettre individuellement à l'analyse antivirus. Les tâches qui, selon les experts de Kaspersky Lab, vous seront les plus utiles sont reprises dans cette section. Il s'agit de la recherche de virus dans les secteurs critiques, parmi les objets de démarrage ainsi que l'analyse complète de l'ordinateur.
La section **Services** contient les fonctions complémentaires de Kaspersky Internet Security. 	Vous pouvez passer à la mise à jour du logiciel, à la consultation des rapports sur le fonctionnement de n'importe quel composant de Kaspersky Internet Security, à la manipulation des objets en quarantaine ou des copies de sauvegarde, à la création d'un disque de secours ou à la fenêtre d'administration des clés de licence.

Section du panneau de navigation de la fenêtre principale	Fonction
La section **Commentaires et conseils** vous accompagne tout au long de l'utilisation du logiciel 	Cette section vous offrira toujours des conseils pour renforcer la protection de l'ordinateur. C'est ici que vous trouverez également les commentaires sur le fonctionnement actuel du logiciel et sur ces paramètres. Grâce aux liens repris dans cette section, vous pouvez accéder directement à l'exécution de l'action recommandée dans un cas concret ou en savoir plus sur les informations.

Chaque élément du panneau de navigation est doté d'un menu contextuel spécial. Ainsi, pour les composants de la protection et les service, ce menu contient des points qui permettent d'accéder rapidement aux paramètres, à l'administration et à la consultation des rapports. Le menu contextuel de la recherche de virus prévoit un point supplémentaire qui vous permet de personnaliser la tâche sélectionnée.

Il est possible également de modifier l'apparence de la fenêtre principale de l'application

4.4. Fenêtre de configuration du logiciel

La fenêtre de configuration de Kaspersky Internet Security peut être ouverte depuis la fenêtre principale (cf. point 4.3, p. 49). Pour ce faire, cliquez sur le lien Configuration dans la partie supérieure.

La fenêtre de configuration (cf. ill. 3) ressemble à la fenêtre principale :

- La partie gauche offre un accès simple et rapide à la configuration de chaque composant du logiciel, des tâches liées à la recherche de virus ainsi qu'à la configuration des services du logiciel;
- La partie droite reprend une énumération des paramètres du composant, de la tâche, etc. sélectionné dans la partie gauche.

Lorsque vous sélectionnez dans la partie gauche de la fenêtre de configuration une section, un composant ou une tâche quelconque, la partie droite affiche les paramètres fondamentaux de l'élément sélectionné. Afin passer à la configuration détaillée de certains paramètres, vous pourrez ouvrir une boîte de

dialogue pour la configuration de deuxième ou de troisième niveau. Une description détaillée des paramètres est offerte dans les sections correspondantes de l'aide électronique.

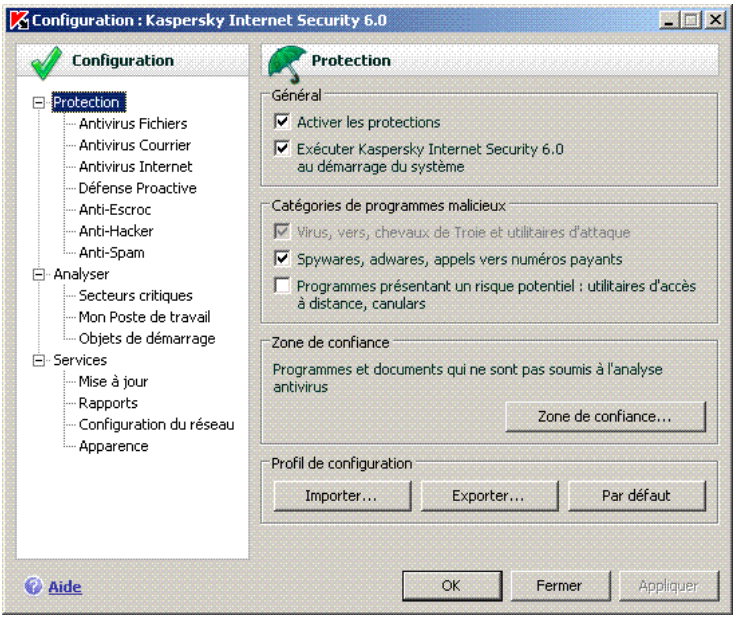


Illustration 3. Fenêtre de configuration de Kaspersky Internet Security

CHAPITRE 5. 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.

Toutefois, les particularités de la configuration de votre ordinateur ou des tâches exécutées peuvent être propres. Pour cette raison, nous vous conseillons de réaliser une configuration préalable du logiciel afin de l'adapter le mieux possible à la protection de votre ordinateur.

Afin de rendre l'utilisation plus conviviale, nous avons tenté de regrouper ces paramètres au sein d'une interface unique : l'assistant de configuration initiale (cf. point 3.2, p. 37). Cet Assistant démarre à la fin de l'installation du logiciel. En suivant les indications de l'Assistant, vous pourrez activer le programme, configurer la mise à jour et le lancement de la recherche de virus, limiter l'accès au programme grâce à un mot de passe et configurer le fonctionnement d'Anti-Hacker selon les caractéristiques de votre réseau.

Une fois que vous aurez installé et lancé le logiciel sur l'ordinateur, nous vous conseillons de réaliser les tâches suivantes :

- Evaluer l'état actuel de la protection (cf. point 5.1, p. 54) pour s'assurer que Kaspersky Internet Security offre le niveau de sécurité souhaité.
- Règles pour l'application (cf. point 5.3, p. 60). pour les logiciels qui requièrent une connexion au réseau.
- Entraîner Anti-Spam sur la base de vos messages (cf. point 5.7, p. 64).
- Mettre à jour le logiciel (au cas où cela n'aurait pas été réalisé à l'aide de l'Assistant de configuration ou automatiquement après l'installation du logiciel) (cf. point 5.8, p. 65).
- Analyser l'ordinateur (cf. point 5.4, p. 62).

5.1. Etat de la protection de l'ordinateur

Toutes les informations relatives à la protection de votre ordinateur sont reprises dans la section **Protection** de la fenêtre principale de Kaspersky Internet Security. Vous y trouverez *l'état actuel de la protection* de l'ordinateur ainsi que des *statistiques générales* sur le fonctionnement du logiciel.

L'**Etat de la protection** illustre l'état actuel de la protection de votre ordinateur à l'aide d'indices spéciaux (cf. point 5.1.1, p. 55). Les statistiques (cf. point 5.1.2, p. 58) affichent les résultats du travail actuel du logiciel.

5.1.1. Indices de protection

L'état de la protection est défini par trois indices qui illustrent le niveau de protection de votre ordinateur à ce moment et qui indiquent tout problème au niveau de la configuration et du fonctionnement du logiciel.

Illustration 4. Indices indiquant l'état de protection de l'ordinateur

L'importance de l'événement signalé par l'indice peut prendre l'une des trois valeurs suivantes :

– *indice informatif* : il signale que la protection de l'ordinateur est au niveau requis et qu'il n'y a aucun problème au niveau de la configuration du logiciel ou du fonctionnement des composants.

– *l'indice attire votre attention sur quelques écarts* dans le fonctionnement de Kaspersky Internet Security par rapport au mode recommandé, ce qui peut avoir une incidence sur la protection de l'information. Veuillez prêter attention aux recommandations des experts de Kaspersky Lab reprises dans la section Commentaires et conseils de la fenêtre principale du logiciel.

 – *l'indice signale une situation critique* au niveau de la protection de votre ordinateur. Suivez scrupuleusement les recommandations fournies dans la section Commentaires et conseils de la fenêtre principale du logiciel. Elles visent toutes à renforcer la protection de votre ordinateur. Les actions recommandées apparaissent sous la forme d'un lien.

Voici une présentation détaillées des indices de protection et des situations dans laquelle ils apparaissent.

Le premier indice illustre une situation impliquant la présence d'objets malveillants sur l'ordinateur. L'indice prend une des valeurs suivantes :

 *Aucun objet malveillant n'a été découvert*

Kaspersky Internet Security n'a découvert aucun objet dangereux sur l'ordinateur.

Tous les objets malveillants ont été neutralisés

Kaspersky Internet Security a réparé tous les objets infectés et supprimés ceux qu'il n'a pas pu réparer.

 *Une attaque de pirates a été bloquée*

Kaspersky Internet Security a découvert et bloqué une tentative d'attaque de réseau.

 *Des objets malveillants ont été découverts*

Votre ordinateur est actuellement exposé à un risque d'infection. Kaspersky Internet Security a découvert des objets malveillants qu'il faut absolument neutraliser. Pour ce faire, cliquez sur Réparer tous. Le lien Détails vous permet d'obtenir de plus amples informations sur les objets malveillants.

Le redémarrage de l'ordinateur est indispensable

Le traitement des objets malveillants requiert le redémarrage de l'ordinateur. Enregistrez et fermez tous les fichiers avec lesquels vous travailliez et cliquez sur Redémarrer l'ordinateur.

Le deuxième indice illustre le degré d'actualité de la protection de l'ordinateur à ce moment. L'indice prend une des valeurs suivantes :

 *Les signatures ont été diffusées (date, heure)*

Le logiciel n'a pas besoin d'être mis à jour. Toutes les bases utilisées par Kaspersky Internet Security contiennent les

informations les plus récentes pour la protection de l'ordinateur.

Les signatures sont dépassées

Les modules de l'application et les bases de données de Kaspersky Internet Security n'ont pas été actualisées depuis quelques jours. Vous risquez d'infecter votre ordinateur avec de nouveaux programmes malveillants ou d'être soumis aux nouvelles attaques apparues depuis la dernière mise à jour de l'application. Il est vivement recommandé de mettre à jour Kaspersky Internet Security. Pour ce faire, cliquez sur Mettre à jour.

Le redémarrage de l'ordinateur est indispensable

La mise à jour correcte du logiciel requiert le redémarrage du système. Enregistrez et fermez tous les fichiers avec lesquels vous travailliez et cliquez sur Redémarrer l'ordinateur.

Les signatures sont dépassées

Il y a longtemps que Kaspersky Internet Security n'a plus été mis à jour. Vous exposez les données de votre ordinateur à un grand risque. Il faut mettre le logiciel à jour le plus vite possible. Pour ce faire, cliquez sur Mettre à jour.

Les signatures sont complètement ou partiellement corrompues

Les fichiers des signatures des menaces sont complètement ou partiellement corrompus. Il est conseillé de lancer à nouveau la mise à jour. Si l'erreur se reproduit, contactez le service d'assistance technique de Kaspersky Lab.

Le troisième indice indique le degré d'utilisation des possibilités du logiciel. L'indice prend une des valeurs suivantes :

Tous les composants de la protection sont actifs

Tous les vecteurs de propagation des programmes malveillants sont protégés par Kaspersky Internet Security Suite. Tous les composants de la protection sont activés.

La protection n'est pas installée

Lors de l'installation de Kaspersky Internet Security, aucun des composants de la protection en temps réel n'a été installé. Le présent mode autorise unique la recherche d'éventuels virus dans les objets. Pour garantir la protection maximale de l'ordinateur, il

est conseillé d'installer les composants de la protection.

Certains composants de la protection sont inactifs

Le fonctionnement d'un ou de plusieurs composants de la protection a été suspendu pour un certain temps. Afin de rétablir le fonctionnement du composant inactif, sélectionnez-le dans la liste et cliquez sur ▶.

Tous les composants de la protection sont inactifs

La protection de l'ordinateur est complètement désactivée. Aucun des composants de la protection ne fonctionne. Pour rétablir le fonctionnement des composants, sélectionnez l'élément **Activation de la protection** dans le menu contextuel qui s'ouvre lorsque vous cliquez sur l'icône de l'application dans la barre des tâches.

Certains composants de la protection sont incorrects

Le fonction d'un ou de plusieurs composants de la protection de Kaspersky Internet Security s'est soldé par un échec. Il est conseillé dans ce cas d'activer le composant ou de redémarrer l'ordinateur (l'enregistrement des pilotes du composant après l'application d'une mise à jour s'impose peut-être).

5.1.2. Etat d'un composant particulier de Kaspersky Internet Security

Pour savoir comment Kaspersky Internet Security protège le système de fichiers, le courrier, le trafic http ou d'autres sources infection potentielle de votre ordinateur, pour suivre l'exécution de la recherche de virus ou de la mise à jour des signatures des menaces, il suffit d'ouvrir la section adéquate dans la fenêtre principale du logiciel.

Ainsi, pour consulter l'état actuel de la protection des fichiers, sélectionnez **Antivirus Fichiers** dans la partie gauche de la fenêtre du programme et pour consulter l'état de la protection contre les nouveaux virus, sélectionnez **Défense proactive**. La partie droite de la fenêtre reprendra des informations de synthèse sur le fonctionnement du composant.

Chaque composant est accompagné d'une **barre d'état**, d'une section **Etat** (**Configuration** pour la recherche de virus et les mises à jour) et d'une section **Statistiques**.

Examinons la *barre d'état* du composant cité dans l'exemple, à savoir Antivirus Fichiers :

- *Antivirus Fichiers : actif* : la protection des fichiers est assurée selon les paramètres du niveau sélectionné. (cf. point 7.1, p. 91).
- *Antivirus Fichiers : pause* : l'antivirus de fichiers a été désactivé pour un temps déterminé. Le composant sera activé automatiquement une fois ce laps de temps écoulé ou après le redémarrage du logiciel. Vous pouvez activer vous-même la protection des fichiers. Pour ce faire, cliquez sur ▶ dans la barre d'état.
- *Antivirus Fichiers* : *inactif*. L'utilisateur a arrêté le composant. Vous pouvez activer la protection des fichiers. Pour ce faire, cliquez sur ▶ dans la barre d'état.
- *Antivirus Fichiers : ne fonctionne pas*. La protection des fichiers est inaccessible pour une raison quelconque. Par exemple, vous ne possédez pas de licence d'utilisation du logiciel.
- *Antivirus Fichiers : échec*. Le composant s'est arrêté suite à un échec. Dans ce cas, contactez le service d'assistance technique de Kaspersky Lab.

Si le composant contient plusieurs modules, la section **Etat** vous renseigne sur l'état du fonctionnement : sont-ils actifs ou pas. Pour les composants qui ne possèdent pas de modules distincts, vous verrez leur propre état, le niveau de protection offert et, pour certains composants, les actions exécutées sur les objets dangereux.

La section **Etat** n'est pas proposée pour les tâches liées à la recherche de virus et à la mise à jour. Le niveau de protection appliqué contre les programmes dangereux lors de l'analyse et le mode de lancement de la mise à jour figure dans le bloc **Configuration**.

Le bloc **Statistiques** contient les résultats du fonctionnement du composant de la protection, de la mise à jour ou de la recherche de virus.

5.1.3. Statistiques

Les statistiques du fonctionnement de l'application sont reprises dans le groupe **Statistique** de la section **Protection** de la fenêtre principale de l'application (cf. ill. 5). Elles fournissent des informations générale sur la protection de l'ordinateur, depuis l'installation de Kaspersky Internet Security.

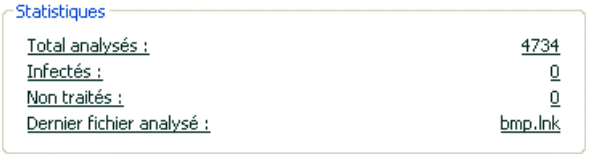


Illustration 5. Bloc des statistiques générales sur le fonctionnement du programme

Un clic du bouton gauche de la souris dans n'importe quel endroit du bloc ouvre un rapport détaillé. Les différents onglets comprennent :

- des informations sur les objets découverts (cf. point 16.3.2, p. 241) et le statut qui leur a été attribué;
- le journal des événements (cf. point 16.3.3, p. 242);
- des statistiques générales sur l'analyse de l'ordinateur (cf. point 16.3.4, p. 243);
- les paramètres de fonctionnement du logiciel (cf. point 16.3.5, p. 244).

Si la recherche de virus est en cours à ce moment, le groupe **Statistiques** affiche une barre de progression de l'analyse.

5.2. Contrôle de l'intégrité de l'application

A cette étape, Kaspersky Internet Security analyse les applications installées sur l'ordinateur (fichiers des bibliothèques dynamiques, signature numérique de l'éditeur), calcule les sommes de contrôle des fichiers des applications et crée une liste de programmes de confiance du point de vue de la sécurité antivirus. Par exemple, cette liste reprendra automatiquement toutes les applications qui possèdent la signature de Microsoft Corporation.

Par la suite, les informations obtenues pendant l'analyse de la structure de l'application seront utilisées par Kaspersky Internet Security pour éviter l'introduction de code malveillant dans le module de l'application.

L'analyse des applications installées sur l'ordinateur peut durer un certain temps.

5.3. Définir les règles de Anti-Hacker

En règle générale, directement après le démarrage du système d'exploitation, plusieurs logiciels de l'ordinateur tentent d'établir une connexion réseau avec certaines ressources. Par exemple, le client de messagerie Microsoft Office

Outlook tente de se connecter au serveur de messagerie afin de télécharger les messages qui vous ont été adressés. ICQ se connecte à Internet afin que vous puissiez entrer en communication avec vos amis et collègues, etc.

Toute l'activité de réseau de votre ordinateur est contrôlée par Kaspersky Anti-Hacker. Les règles de Kaspersky Anti-Hacker pour la majorité des applications système qui requièrent une connexion au réseau sont déjà définies et intégrées à Kaspersky Internet Security. Si cette règle n'existe pas, Anti-Hacker vous avertit qu'il a découvert un programme qui tente de se connecter à une ressource réseau quelconque.

Si votre ordinateur se connecte au réseau lors du démarrage, le programme vous en avertit et vous demande si ce réseau est fiable.

Les messages relatifs à l'activité de certains programmes sur votre ordinateur (cf. ill. 6) contiennent de brèves informations sur la connexion et les actions possibles par rapport à ce programme :

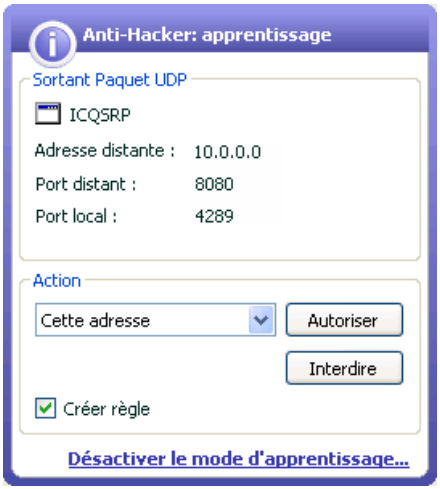


Illustration 6. Notification d'Anti-Hacker sur la découverte d'une activité de réseau d'ICQ

- Autoriser l'activité de réseau.
- Interdire l'activité de réseau.
- Réaliser une configuration plus détaillée de Kaspersky Internet Security par rapport à ce programme.

Afin qu'Anti-Hacker se souvienne de l'action que vous avez sélectionnée, cochez la case ☑ **Créer règle**. Le composant n'affichera plus le message lorsqu'il détectera une tentative de connexion de ce programme à la ressource indiquée selon les paramètres définis.

Si vous souhaitez créer des règles pour les logiciels installés sur votre ordinateur ultérieurement, cliquez sur Désactiver le mode d'apprentissage. Dans ce cas, Anti-Hacker entrera en mode de protection minimale et les tentatives de connexion au réseau réalisées par le logiciel, de chargement ou de transfert des paquets de données depuis le réseau seront autorisées.

5.4. Recherche d'éventuels virus

Les experts de Kaspersky Lab vous conseillent vivement de rechercher régulièrement la présence d'éventuels virus sur votre ordinateur. Dès que l'installation est terminée, un message spécial vous signale que l'analyse de l'ordinateur n'a pas encore été réalisée et qu'il est conseillé de la lancer immédiatement.

Kaspersky Internet Security possède par défaut une tâche de recherche de virus sur l'ordinateur. Elle se trouve dans la section **Analyser** de la fenêtre principale du logiciel.

Après avoir sélectionné la tâche **Mon poste de travail** dans la partie gauche de la fenêtre principale, vous pouvez consulter les statistiques de la dernière analyse et les paramètres de la tâche : le niveau de protection sélectionnée et l'action exécutée sur les objets dangereux.

Pour rechercher la présence d'éventuels objets malveillants sur l'ordinateur :

cliquez sur **Analyser** dans la partie droite de la fenêtre.

Cette action lancera l'analyse de l'ordinateur et les détails de celle-ci sont repris dans une fenêtre spéciale. Vous pouvez cacher la fenêtre reprenant les informations relatives à l'exécution de la tâche en la refermant tout simplement. L'analyse ne sera pas interrompue.

5.5. Recherche d'éventuels virus dans les secteurs critiques de l'ordinateur

Il existe sur votre ordinateur des secteurs critiques du point de vue de la sécurité. Ils sont infectés par les programmes malveillants qui veulent endommager le système d'exploitation, le processeur, la mémoire, etc.

Il est primordial de protéger les secteurs critiques de l'ordinateur afin de préserver leur fonctionnement. Une tâche spéciale a été configurée pour rechercher d'éventuels virus dans ces secteurs. Elle se trouve dans la section **Recherche de virus** de la fenêtre principale du logiciel.

Après avoir sélectionné la tâche **Secteurs critiques** dans la partie gauche de la fenêtre principale, vous pouvez consulter les statistiques de la dernière analyse et les paramètres de la tâche : le niveau de protection sélectionné et l'action exécutée sur les objets malveillants. Il est possible de sélectionner également les

secteurs critiques précis que vous souhaitez analyser et lancer directement l'analyse antivirus de ceux-ci.

Pour rechercher la présence d'éventuels objets malveillants dans les secteurs critiques de l'ordinateur :

cliquez sur **Analyser** dans la partie droite de la fenêtre.

Cette action lancera l'analyse des secteurs choisis et les détails de celle-ci sont repris dans une fenêtre spéciale. Vous pouvez cacher la fenêtre reprenant les informations relatives à l'exécution de la tâche en la refermant tout simplement. L'analyse ne sera pas interrompue.

5.6. Recherche d'éventuels virus dans les fichiers, les répertoires ou les disques

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

Pour lancer l'analyse d'un objet :

Placez la souris sur l'objet, ouvrez le menu contextuel de Microsoft Windows d'un clic droit et sélectionnez **Rechercher d'éventuels virus** (cf. ill. 7).

Illustration 7. Recherche d'éventuels virus dans un objet sélectionné à l'aide des outils Windows

Cette action lancera l'analyse de l'objet choisi et les détails de celle-ci sont repris dans une fenêtre spéciale. Vous pouvez cacher la fenêtre reprenant les informations relatives à l'exécution de la tâche en la refermant tout simplement. L'analyse ne sera pas interrompue.

5.7. Entraînement d'Anti-Spam

Une des étapes des travaux préparatifs consiste à apprendre à Anti-Spam à travailler avec les messages que vous recevez. Le problème du courrier indésirable est qu'il est très difficile de définir ce qui constitue un message non sollicité pour un utilisateur particulier. Il existe bien entendu des catégories de messages qui peuvent être classés avec certitude dans la catégorie du courrier indésirable (publipostage, publicité, message avec des caractères orientaux), toutefois ce type de messages peut être utile pour certains utilisateurs.

C'est la raison pour laquelle nous vous proposons de définir vous-même les catégories de courrier indésirable. Après l'installation, Kaspersky Internet Security vous propose d'entraîner Anti-Spam à faire la différence entre le courrier indésirable et le courrier normal. Pour ce faire, il vous suffit d'utiliser les boutons spéciaux intégrés à votre client de messagerie (Microsoft Office Outlook, Microsoft Outlook Express et TheBat!) ou l'Assistant d'apprentissage spécial.

Pour entraîner Anti-Spam à l'aide des boutons spéciaux :

1. Ouvrez le client de messagerie utilisé par défaut sur votre ordinateur, par exemple Microsoft Office Outlook. Vous voyez les deux boutons suivants dans la barre d'outils : **Courrier indésirable** et **Courrier normal**.

2. Sélectionnez un message normal, un groupe de messages ou un dossier contenant des messages normaux et cliquez sur **Courrier normal**. Désormais, les messages en provenance des expéditeurs des messages sélectionnés seront toujours considérés comme du courrier normal.

3. Sélectionnez un message qui contient des informations qui ne vous sont pas utiles ou un groupe ou un dossier contenant de tels messages et cliquez sur **Courrier indésirable**. Anti-Spam analyse le contenu de ces messages et à l'avenir tous les messages au contenu similaire seront plus que vraisemblablement associé au courrier indésirable.

Pour entraîner Anti-Spam à l'aide de l'Assistant spécial :

1. Sélectionnez le composant Anti-Spam dans la section **Protection** de la fenêtre principale du logiciel et cliquez sur le lien **Configuration**.

2. Dans la partie droite de la fenêtre de configuration cliquez sur **Assistant d'apprentissage**.
3. Au cours de la première étape, sélectionnez les dossiers de votre client de messagerie qui contiennent du courrier utile. Cliquez sur **Suivant**.
4. Au cours de la deuxième étape, sélectionnez les dossiers contenant le courrier indésirable. Cliquez sur **Suivant**.

L'entraînement est réalisé sur la base des dossiers que vous avez indiqués.

Lorsqu'un message arrive dans votre boîte aux lettres, Anti-Spam vérifie s'il s'agit d'un message non sollicité et ajoute le texte [Spam] à l'objet du message si celui-ci est considéré comme un message non sollicité. Vous pouvez établir une règle pour ces messages dans le client de messagerie qui les supprimera ou les classera dans un dossier spécial.

5.8. Mise à jour du logiciel

Kaspersky Lab met à jour les signatures des menaces et les modules de Kaspersky Internet Security via des serveurs spéciaux de mise à jour.

Les serveurs de mises à jour de Kaspersky Lab sont les sites Internet que Kaspersky Lab utilise pour diffuser les mises à jour du logiciel.

Attention !

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

Kaspersky Internet Security vérifie automatiquement la présence des mises à jour sur les serveurs de Kaspersky Lab. Si Kaspersky Lab a diffusé des mises à jour pour le logiciel, Kaspersky Internet Security les télécharge et les installe en arrière plan.

Pour procéder à la mise à jour manuelle de Kaspersky Internet Security :

Sélectionnez le composant **Mise à jour** dans la section **Service** de la fenêtre principale du logiciel et cliquez sur **Mettre à jour** dans la partie droite.

Cette action entraînera la mise à jour de Kaspersky Internet Security. Tous les détails du processus sont illustrés dans une fenêtre spéciale.

5.9. Que faire des objets dangereux

Un message spécial s'affiche en cas de découverte d'objets dangereux dans votre courrier, dans les fichiers ouverts ou dans les programmes exécutés (cf. ill. 8).

Illustration 8. Notification de la découverte d'un virus

Voici les types de message prévus :

- *Attention* : un objet suspect a été découvert. Lorsque cela est possible, le nom du programme dangereux infecte peut-être le fichier est affiché.
- *Alerte* : un objet malveillant a été découvert.

La notification contient :

- Le nom du programme malveillant qui a infecté l'objet. Ce nom apparaît sous la forme d'un lien vers le site http://www.viruslist.com/fr où vous pourrez obtenir de plus amples informations sur le type de menace découvert sur votre ordinateur.
- Le nom complet de l'objet dangereux.
- Un bref résumé et sélection des actions éventuelles à exécuter sur l'objet. Le résumé indique le type de programme malveillant qui a infecté l'objet et précise s'il est possible de le neutraliser.

Si l'objet peut être réparé, vous aurez le choix entre l'une des actions suivantes :

- **Réparer** : tentative de réparation de l'objet infecté. Une copie de sauvegarde est créée avant la réparation au cas où il faudra restaurer l'objet ou le scénario de l'infection.

- **Supprimer** : suppression de l'objet. Une copie de sauvegarde est créée avant la suppression au cas où il faudra restaurer l'objet ou le scénario de l'infection.
- **Ignorer** : aucune action n'est réalisée, seules les informations sont consignées dans le rapport. Si cette action est sélectionnée, l'objet sera à nouveau accessible et la copie sera conservée dans le dossier de sauvegarde.

S'il est impossible de réparer l'objet, Kaspersky Internet Security propose de le supprimer ou de l'ignorer.

Si l'objet est soupçonné d'être infecté, vous pouvez soit le supprimer, soit l'ignorer ou soit le placer en quarantaine.

Pour exécuter l'action, il suffit de cliquer sur le bouton correspondant.

Vous pouvez appliquer l'action sélectionnée à tous les objets à l'état identique découverts lors de la même session. Pour ce faire, cochez la case ☑ **Appliquer à tous les cas identiques**.

Il est possible que l'objet dangereux suspect découvert ne représente en fait aucun risque pour vous. Imaginez par exemple que vous avez créé un fichier considéré comme dangereux par le logiciel alors que vous savez pertinemment bien que ce n'est pas le cas. Vous utilisez ce fichier en permanence et vous savez qu'il ne peut en aucun cas nuire à votre ordinateur. Dans ce cas, il est recommandé d'ajouter ce fichier à la liste des exclusions. Cela peut se faire au départ d'une fenêtre spéciale (cf. point 6.3, p. 75) ou directement depuis la fenêtre de notification en cliquant sur Ajouter à la zone de confiance.

5.10. Que faire si la protection ne fonctionne pas

En cas de problème ou d'erreur de fonctionnement d'un composant quelconque de la protection, veuillez vérifier son état.

Si l'état donné est *<nom du composant> : ne fonctionne pas* ou *<nom du composant>: échec*, essayez de redémarrer le logiciel.

Si le problème n'est pas résolu après le redémarrage du logiciel, nous vous conseillons de contacter le Service d'assistance technique. Veuillez au préalable enregistrer le rapport du composant dans un fichier et envoyez-le à Kaspersky Lab. Cela permettra aux opérateurs du Service d'assistance technique de comprendre votre problème.

Afin d'enregistrer le rapport dans un fichier :

1. Sélectionnez le composant dans la section **Protection** de la fenêtre principale du logiciel et cliquez avec le bouton gauche de la souris n'importe où dans le bloc **Statistiques**.
2. Cliquez sur **Enregistrer sous** et saisissez, dans la fenêtre qui s'ouvre, le nom du fichier dans lequel vous souhaitez enregistrer les résultats du fonctionnement du composant.

Afin d'enregistrer directement le rapport de tous les composants de Kaspersky Internet Security (composants de la protection, tâches de recherche de virus, fonctions de services),

1. Sélectionnez la section **Protection** dans la fenêtre principale du logiciel et cliquez avec le bouton gauche de la souris n'importe où dans le bloc **Statistiques**.

   ou

   Dans la fenêtre du rapport de n'importe quel composant, cliquez sur le lien Liste de tous les rapports. Les rapports pour tous les composants de l'application seront repris dans l'onglet **Rapport**.
2. Cliquez sur **Enregistrer sous** et indiquez, dans la fenêtre qui s'ouvre, le nom du fichier dans lequel les résultats du fonctionnement du programme seront conservés.

CHAPITRE 6. ADMINISTRATION COMPLEXE DE LA PROTECTION

Kaspersky Internet Security peut être soumis à une administration complexe :

- Désactivation/activation du logiciel (cf. point 6.1, p. 69).
- Sélection des logiciels contrôlés contre lesquels Kaspersky Internet Security vous protégera (cf. point 6.2, p. 74).
- Constitution de la liste des exclusions pour la protection (cf. point 6.3, p. 75).
- Création de tâches personnalisées de recherche de virus et de mise à jour (cf. point 6.4, p. 84).
- Configuration du lancement des tâches à l'heure qui vous convient (cf. point 6.5, p. 85).
- Importation et exportation des paramètres de fonctionnement du logiciel (cf. point 6.4, p. 88)

6.1. Désactivation/activation de la protection de votre ordinateur

Par défaut, Kaspersky Internet Security est lancé au démarrage du système comme en témoigne le message *Protégé par Kaspersky Internet Security* qui apparaît dans le coin supérieur droit de l'écran. La protection est garantie pendant toute la séance de travail. Tous les composants de la protection sont activés (cf. point 2.2.1, p. 26).

Vous pouvez désactiver la protection offerte par Kaspersky Internet Security soit complètement, soit partiellement.

Attention !

Les experts de Kaspersky Lab vous recommandent vivement de **ne pas désactiver la protection** car cela pourrait entraîner l'infection de l'ordinateur et la perte de données.

Notez que dans ce cas, la protection est envisagée dans le contexte des composants du logiciel. La désactivation ou la suspension du fonctionnement des composants du logiciel n'a pas d'influence sur la recherche de virus et la mise à jour du logiciel.

6.1.1. Suspension de la protection

La suspension signifie que tous les composants de la protection qui vérifient les fichiers sur votre ordinateur, le courrier entrant et sortant, les scripts exécutés et le comportement des applications sont désactivés, tout comme Anti-Hacker et Anti-Spam.

Pour suspendre le fonctionnement de Kaspersky Internet Security :

1. Sélectionnez **Suspension de la protection** dans le menu contextuel (cf. point 4.2, p. 48)
2. Dans la fenêtre de désactivation (cf. ill. 9), sélectionnez la durée au terme de laquelle la protection sera réactivée :
   - **Dans X minutes/heures** : la protection sera activée au terme de l'intervalle indiqué.
   - **Lors de la connexion à Internet** : la protection sera activée directement après la connexion de l'ordinateur au réseau.
   - **Après le redémarrage du logiciel :** la protection sera activée si vous lancez le programme depuis le menu **Démarrer** ou après le redémarrage du système (pour autant que le lancement du programme au démarrage du système d'exploitation soit activé (cf. point 6.1.5, p. 73).
   - **Jamais** : la protection sera activée uniquement lorsque vous le déciderez. Pour activer la protection, cliquez sur le point **Activation de la protection** dans le menu contextuel du programme.

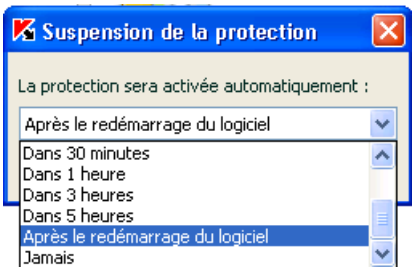


Illustration 9. Fenêtre de suspension de la protection de votre ordinateur

Astuce.

Vous pouvez également désactiver la protection de votre ordinateur jusqu'au prochain redémarrage du système de l'une des deux méthodes suivantes :

- Cliquez sur dans la section **Protection**.
- Sélectionnez **Quitter** dans le menu contextuel. Le programme sera déchargé de la mémoire vive.

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 grisé dans la section **Protection** de la fenêtre principale.
- L'icône de l'application dans la barre des tâches est en noir et blanc.
- Le troisième indice de protection (cf. point 5.1.1, p. 55) de votre ordinateur indique *Tous les composants de la protection sont inactifs*.

6.1.2. Désactivation complète de la protection de l'ordinateur

La désactivation complète signifie l'arrêt du fonctionnement des composants de la protection. La recherche des virus et la mise à jour se poursuivent dans ce mode.

Si la protection est totalement désactivée, elle ne pourra être réactivée qu'à la demande de l'utilisateur. L'activation automatique des composants de la protection après le redémarrage du système ou du logiciel n'aura pas lieu dans ce cas. Si pour une raison quelconque Kaspersky Internet Security entre en conflit avec d'autres logiciels installés sur l'ordinateur, vous pouvez arrêter le fonctionnement de composants individuels ou composer une liste d'exclusions (cf. point 6.3, p. 75).

Pour désactiver complètement la protection de l'ordinateur :

1. Ouvrez la fenêtre principale de Kaspersky Internet Security.
2. Cliquez sur le Configuration dans la section **Protection**.
3. Dans la fenêtre des paramètres du logiciel, désélectionnez la case **Activer les protections**.

Cette action entraînera l'arrêt du fonctionnement de tous les composants. Les éléments suivants permettent de confirmer la désactivation :

- Le nom des composants désactivés apparaît en grisé dans la section **Protection** de la fenêtre principale.
- L'icône de l'application dans la barre des tâches est en noir et blanc.
- L'indice de la protection (cf. point 5.1.1, p. 55) de votre ordinateur indique *Tous les composants de la protection sont inactifs*.

6.1.3. Suspension / désactivation du composant de la protection, de la recherche de virus ou de la mise à jour

Il existe plusieurs moyens de désactiver un composant de la protection ou une tâche liée à la mise à jour ou à la recherche de virus. Toutefois, avant de faire quoi que ce soit, nous vous conseillons de définir la raison pour laquelle vous souhaitez les suspendre. Le problème pourrait également être résolu en modifiant, par exemple, le niveau de protection. Ainsi, si vous utilisez une base de données qui selon vous ne peut contenir de virus, il suffit de reprendre ce répertoire et les fichiers qu'il contient dans les exclusions (cf. point 6.3, p. 75).

Pour suspendre un composant de la protection, la recherche de virus ou la mise à jour

Sélectionnez le composant ou la tâche dans la section correspondante de la partie gauche de la fenêtre principale du logiciel et cliquez sur dans la barre d'état.

L'état du composant (de la tâche) passe à *pause*. La protection assurée par le composant ou la tâche qui était exécutée sera suspendue jusqu'à ce que vous la réactiviez en cliquant sur le bouton .

Pour arrêter un composant, la recherche de virus ou la mise à jour :

Cliquez sur dans la barre d'état. Vous pouvez également arrêter un composant dans la boîte de dialogue de configuration du programme en désélectionnant la case **Activer <nom du composant>** dans le bloc **Général** du composant en question.

Dans ce cas, l'état du composant (tâche) devient *désactivé (interrompu)*. La protection assurée par le composant ou la tâche qui était exécutée sera arrêtée jusqu'à ce que vous la réactiviez en cliquant sur le bouton .

Pour la recherche de virus et la mise à jour, vous aurez le choix entre les options suivantes : poursuivre l'exécution de la tâche interrompue ou la reprendre à zéro.

La différence entre ces deux méthodes de désactivation du composant est la suivante :

- Quand vous suspendez un composant ou l'exécution d'une tâche (bouton), les statistiques relatives à la session en cours de Kaspersky Internet Security sont conservées et reprendront après le rétablissement du travail.
- Lorsque vous arrêtez la protection (bouton), toutes les statistiques sont remises à zéro et reprendront au redémarrage du composant. .

6.1.4. Rétablissement de la protection de l'ordinateur

Si vous avez à un moment quelconque arrêté ou suspendu la protection de l'ordinateur, vous pourrez la rétablir à l'aide de l'une des méthodes suivantes :

- *Au départ du menu contextuel*.

  Sélectionnez le point **Activation la protection**.

- *Au départ de la fenêtre* **principale** *du logiciel*.

  Cliquez sur dans la barre d'état de la section **Protection** dans la fenêtre principale

L'état de la protection redevient immédiatement *fonctionne*. L'icône du logiciel dans la barre des tâches redevient active (en couleur). Le troisième indice de protection (cf. point 5.1.1, p. 55) de l'ordinateur indique **Tous les composants de la protection sont actifs**.

6.1.5. Fin de l'utilisation du logiciel

Si pour une raison quelconque vous devez arrêter d'utiliser Kaspersky Internet Security, sélectionnez le point **Quitter** dans le menu contextuel (cf. point 4.2, p. 48) du programme. Celui-ci sera déchargé de la mémoire vive, ce qui signifie que votre ordinateur ne sera plus protégé à partir de ce moment.

Au cas où des connexions contrôlées par le logiciel seraient établies lorsque vous arrêtez d'utiliser l'ordinateur, un message s'affichera pour indiquer la déconnexion. Ceci est indispensable pour quitter correctement le programme. La déconnexion s'opère automatiquement après 10 secondes ou lorsque vous

cliquez sur **Oui**. La majorité des connexions interrompues seront rétablies automatiquement après un certain temps.

N'oubliez pas que si vous téléchargez un fichier sans l'aide d'un gestionnaire de téléchargement au moment de la déconnexion, le transfert des données sera interrompu. Vous devrez reprendre le téléchargement du fichier à zéro.

Vous pouvez annuler la déconnexion. Pour ce faire, cliquez sur **Non** dans la fenêtre d'avertissement. Le logiciel continuera à fonctionner.

Si vous avez quitté le logiciel, sachez que vous pouvez à nouveau activer la protection de l'ordinateur en lançant Kaspersky Internet Security au départ du menu **Démarrer → Programmes → Kaspersky Internet Security 6.0 → Kaspersky Internet Security 6.0**.

Il est possible également de lancer la protection automatiquement après le redémarrage du système d'exploitation. Afin d'activer ce mode, passez à la section **Protection** et cochez la cas ☑ **Lancer Kaspersky Internet Security 6.0 au démarrage du système**.

6.2. Sélection des programmes malveillants contrôlés

Kaspersky Internet Security vous protège contre divers types de programmes malveillants. Quelle que soit la configuration du programme, les virus, les chevaux de Troie et les programmes d'attaque informatique sont toujours décelés et neutralisés. Il s'agit des programmes qui peuvent occasionner les dégâts les plus graves. Afin de garantir une plus protection plus étendue, vous pouvez agrandir la liste des menaces à découvrir en activant la recherche de divers programmes qui présentent un risque potentiel.

Afin de sélectionner les types de programmes malveillants contre lesquels Kaspersky Internet Security vous protégera, passez à la section **Protection**, de la fenêtre de configuration du logiciel (cf. point 4.4, p. 52).

Les types de menaces (cf. point 1.2, p. 11) figurent dans le bloc **Catégories de programmes malicieux** :

☑ **Virus, vers, chevaux de Troie et utilitaires d'attaque**. Ce groupe reprend les programmes malveillants les plus répandus et les plus dangereux. Cette protection est le niveau minimum admissible et la désactivation augmente sensiblement la probabilité d'infection de votre ordinateur. Conformément aux recommandations des experts de Kaspersky Lab, il est impossible d'exclure ces objets du cadre des objets contrôlés par Kaspersky Internet Security.

- **Spywares, Adwares, Appels vers numéros payants**. Ce groupe recouvre tous les riskwares qui peuvent être à l'origine d'une influence dangereuse.
- **Programmes présentant un risque potentiel : utilitaires d'administration à distance, jokes**. Ce groupe reprend les logiciels qui ne sont pas malveillants ou dangereux mais qui dans certaines circonstances peuvent servir à endommager votre ordinateur.

Ces groupes règlent l'ensemble de l'utilisation des signatures de menaces lors de l'analyse d'objets en temps réel ou lors de la recherche d'éventuels virus sur votre ordinateur.

Lorsque tous les groupes sont sélectionnés, Kaspersky Internet Security garantit la protection antivirus maximale de votre ordinateur. Si le deuxième et le troisième groupe sont désélectionnés, le logiciel vous protège uniquement contre les objets malveillants les plus répandus sans prêter attention aux programmes dangereux ou autres qui pourraient être installés sur votre ordinateur et causer des dommages matériels ou moraux.

Les experts de Kaspersky Lab vous recommandent de désactiver le contrôle des groupes de menaces uniquement lorsque cela est absolument nécessaire. Si vous souhaitez par exemple désactiver le contrôle des riskwares du deuxième groupe parce que Kaspersky Internet Security vous gênera dans l'utilisation de certaines applications qu'il considèrera comme un programme présentant un risque potentiel, il vous suffira dans ce cas de l'ajouter à la liste des exclusions (cf. point 6.3, p. 75).

6.3. Constitution de la zone de confiance

La Zone de confiance est en réalité une liste d'objets composée par l'utilisateur. Ces objets seront ignorés par Kaspersky Internet Security. En d'autres termes, il s'agit des éléments exclus de la protection offerte par le programme.

Cette zone de confiance peut être définie par l'utilisateur sur la base des particularités des objets qu'il manipule et des programmes installés sur l'ordinateur. La constitution de cette liste d'exclusions peut s'avérer utile si Kaspersky Internet Security bloque l'accès à un objet ou un programme quelconque alors que vous êtes convaincu que celui-ci est tout à fait sain.

Il est possible d'exclure des fichiers d'un certain format, des fichiers selon un masque, certains secteurs (par exemple, un répertoire ou un programme), des processus ou des objets en fonction d'un verdict (état attribué à l'objet par le programme suite à l'analyse).

Afin de composer une liste des exclusions de la protection :,

1. Ouvrez la fenêtre de configuration de Kaspersky Internet Security et passez à la section **Protection**.
2. Cliquez sur **Zone de confiance** dans le bloc du même nom.
3. Dans la boîte de dialogue (cf. ill. 10) qui apparaît, configurer les règles d'exclusion pour les objets et composez également une liste d'applications de confiance.

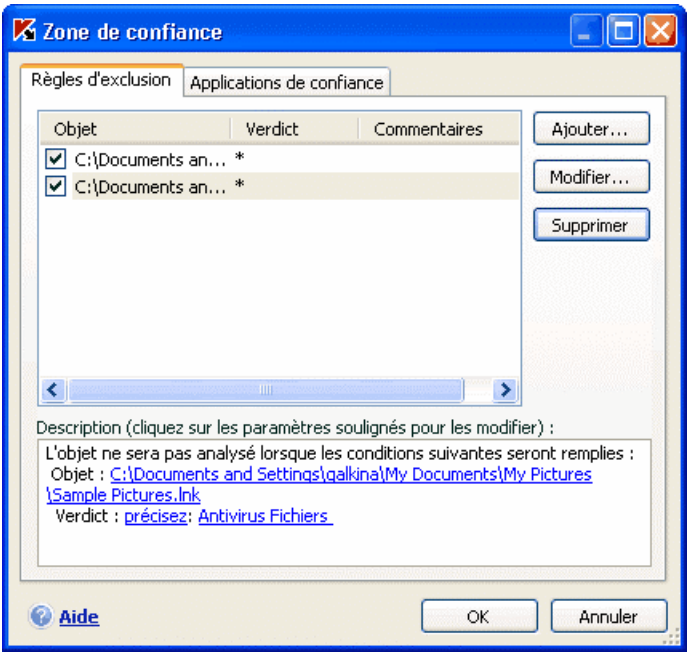


Illustration 10. Constitution de la zone de confiance

6.3.1. Règles d'exclusion

La règle d'exclusion est un ensemble de paramètres qui détermine si un objet quelconque sera analysé ou non par Kaspersky Internet Security

Vous pouvez exclure de l'analyse des fichiers d'un format défini, des fichiers selon un masque, certains secteurs (par exemple : un répertoire ou un programme), des processus ou des objets selon un verdict

Le verdict est l'état que Kaspersky Internet Security a attribué à un objet après l'analyse. Le verdict est rendu sur la base du classement des programmes

malveillants et des riskwares présentés dans l'encyclopédie des virus de Kaspersky Lab.

Les riskwares n'ont pas de fonction malveillante mais ils peuvent être utilisés en tant que "complice" d'autres programmes malveillants car il présentent des failles et des erreurs. Les programmes d'administration à distance, les clients IRC, les serveurs FTP, tous les utilitaires d'arrêt ou de dissimulation de processus, les détecteurs de frappe de clavier, les décrypteurs de mot de passe, les dialers, etc. appartiennent à cette catégorie. Un tel programme n'est pas considéré comme un virus (not-a-virus) mais il peut appartenir à un sous-groupe tel que Adware, Joke, Riskware, etc. (pour obtenir de plus amples informations sur les programmes malveillants découverts par Kaspersky Internet Security, consultez l'encyclopédie des virus à l'adresse www.viruslist.com/fr). De tels programmes peuvent être bloqués après l'analyse. Dans la mesure où certains d'entre eux sont très populaires auprès des utilisateurs, il est possible de les exclure de l'analyse. Pour ce faire, il faut indiquer le verdict attribué à ce programme parmi les exclusions.

Admettons que vous utilisiez souvent Remote Administrator. Il s'agit d'un système d'accès à distance qui permet de travailler sur un ordinateur distant. Kaspersky Internet Security classe cette activité parmi les activités qui présentent un risque potentiel et peut la bloquer. Afin d'éviter le blocage de l'application, il faut composer une règle d'exclusion pour laquelle le verdict sera Remote Admin.

L'ajout d'une exclusion s'accompagne de la création d'une règle qui pourra être exploitée par certains composants du programme (Antivirus Fichiers, Antivirus Courrier, Défense proactive) et lors de l'exécution de tâches liées à la recherche de virus. Vous pouvez composer la règle dans une boîte de dialogue spéciale accessible au départ de la fenêtre de configuration de l'application, au départ de la notification de la découverte d'un objet ou au départ de la fenêtre du rapport.

*Ajout d'exclusion sur l'onglet **Règles d'exclusion** :*

1. Cliquez sur **Ajouter** dans la fenêtre **Règles d'exclusion**.
2. Dans la fenêtre qui apparaît (cf. ill. 11), sélectionnez le type d'exclusion dans la section **Paramètres** :

   - **Objet** : exclusion de l'analyse d'un objet, d'un répertoire particulier ou de fichiers correspondant à un masque défini.
   - **Verdict :** exclusion de l'analyse d'un objet sur la base d'un état attribué selon le classement de l'encyclopédie des virus.

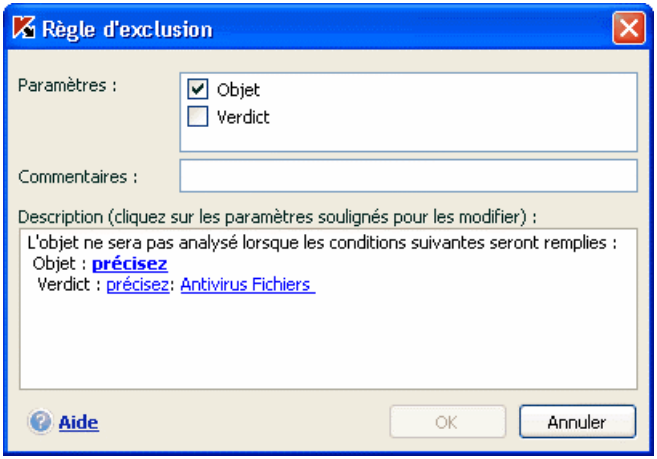


Illustration 11. Création d'une règle d'exclusion

Si vous cochez simultanément les deux cases, vous créerez une règle pour l'objet défini répondant au verdict sélectionné. Dans ce cas, les règles suivantes entreront en application :

- Si un fichier quelconque a été défini en tant qu' **Objet** et qu'un état particulier a été sélectionné pour le **Verdict**, cela signifie que le fichier sélectionné sera exclu uniquement si l'état défini lui sera attribué pendant l'analyse.
- Si un secteur ou un répertoire quelconque a été défini en tant qu'**Objet** et qu'un état (ou masque de verdict) a été défini en tant que **Verdict**, cela signifie que les objets correspondant à cet état, mais découverts uniquement dans ce secteur/répertoire, seront exclus.

3. Définissez la valeur du type d'exclusion sélectionné. Pour ce faire, cliquez avec le bouton gauche de la souris dans la section **Description** sur le lien précisez, situé à côté du type d'exclusion :

   - Pour le type **Objet**, saisissez dans la fenêtre qui s'ouvre son nom (il peut s'agir d'un fichier, d'un répertoire quelconque ou d'un masque de fichiers (cf. point A.2, p. 292). Afin que l'objet indiqué (fichier, masque de fichiers, répertoire) soit ignoré partout pendant l'analyse, cochez la case ☑ **Sous-répertoires compris**. Si vous avez défini le fichier **C:\Program Files\winword.exe** comme une exclusion et que vous avez coché la case d'analyse des sous-répertoire, le fichier **winword.exe** situé dans n'importe quel sous-répertoire de **C:\Program Files** sera ignoré.

- Pour le **Verdict** indiquez le nom complet de l'exclusion telle qu'elle est reprise dans l'encyclopédie des virus ou selon un masque (cf. point A.3, p. 293).

  Pour certains verdicts, il est possible de définir dans le champ **Paramètres complémentaires** des conditions supplémentaires pour l'application de l'exclusion. Dans la majorité des cas, ce champ est rempli automatiquement lors de l'ajout d'une règle d'exclusion au départ de la notification de la défense proactive.

  La saisie de paramètres complémentaires est requise pour les verdicts suivants :

  - *Invader* (intrusion dans les processus du programme). Pour ce verdict, vous pouvez définir en guise de condition d'exclusion complémentaire le nom, le masque ou le chemin d'accès complet à l'objet victime de l'intrusion (par exemple, un fichier dll).
  - *Launching Internet Browser* (lancement du navigateur selon les paramètres). Pour ce verdict, vous pouvez définir en guise de condition d'exclusion complémentaire les paramètres de lancement du navigateur. Par exemple, vous avez interdit le lancement du navigateur selon les paramètres dans l'analyse de l'activité des applications de la Défense proactive. Vous souhaitez toutefois autoriser le lancement du navigateur pour le domaine *www.kaspersky.com* au départ d'un lien dans Microsoft Office Outlook. Pour ce faire, sélectionnez Microsoft Office Outlook en tant qu'**Objet** de l'exclusion et *Launching Internet Browser* en tant que **Verdict**. Dans le champ **Paramètres complémentaires**, saisissez le masque du domaine autorisé.

4. Définissez les composants de Kaspersky Internet Security qui exploiteront la règle ainsi créée. Si vous choisissez la valeur quelconque, cette règle sera exploitée par tous les composants. Si vous souhaitez limiter l'application de cette règle à quelques composants uniquement, cliquez à nouveau sur quelconque et le lien prendra la valeur indiqué. Dans la fenêtre qui s'ouvre, cochez la case en regard des composants qui exploiteront la règle d'exclusion.

Création d'une règle d'exclusion au départ de la notification de la découverte d'un objet dangereux :

1. Cliquez sur Ajouter à la liste de confiance dans la fenêtre de notification (cf. ill. 12).

Illustration 12. Notification sur la découverte d'un objet dangereux

2. Dans la boîte de dialogue qui s'affiche, vérifiez si tous les paramètres vous conviennent. Les champs reprenant le nom de l'objet et le type de menace attribué sont remplis automatiquement sur la base des renseignements qui figurent dans la notification. Afin de créer une règle, cliquez sur **OK**.

Création d'une règle d'exclusion au départ de la fenêtre du rapport :

1. Sélectionnez dans le rapport l'objet que vous souhaitez ajouter aux exclusions.
2. Ouvrez le menu contextuel et sélectionnez le point **Ajouter à la zone de confiance** (cf. ill. 13).
3. Cette action entraîne l'ouverture de la fenêtre de configuration des exclusions. Vérifiez si tous les paramètres vous conviennent. Les champs reprenant le nom de l'objet et le type de menace attribué sont remplis automatiquement sur la base des renseignements qui figurent dans la notification. Afin de créer une règle, cliquez sur **OK**.

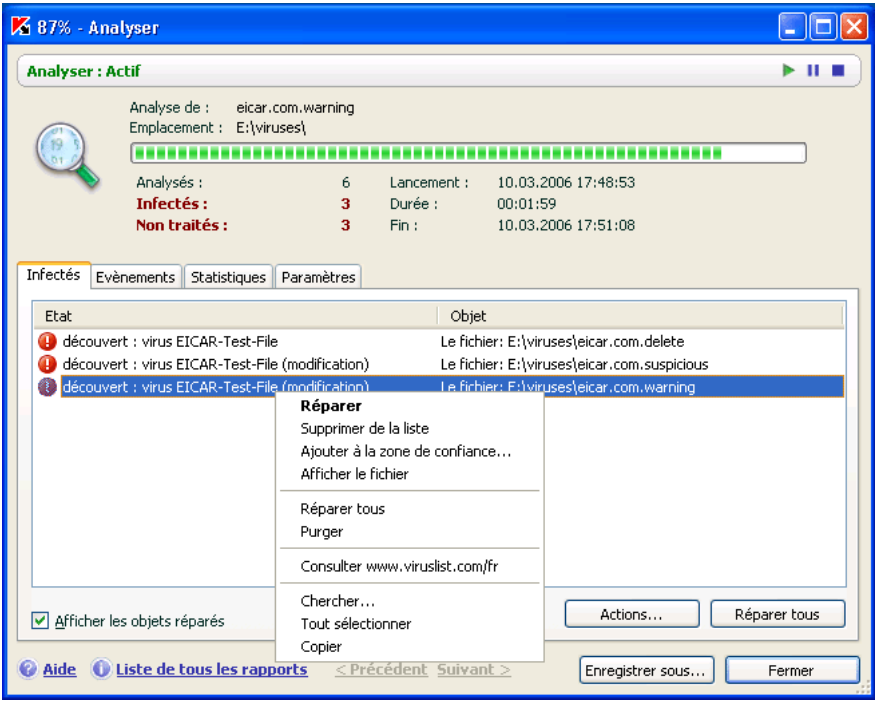


Illustration 13. Création d'une règle d'exclusion au départ du rapport

6.3.2. Applications de confiance

Kaspersky Internet Security vous permet de créer une liste d'applications de confiance dont l'activité, y compris les activités suspectes, les activités de fichiers, les activités de réseau et les requêtes adressées à la base de registre système ne sera pas contrôlée.

Par exemple, vous estimez que le objets utilisés par le programme **Bloc-notes** de Microsoft Windows sont inoffensifs et n'ont pas besoin d'être analysés. En d'autres termes, vous faites confiance aux processus de ce programme. Afin d'exclure de l'analyse les objets utilisés par ce processus, ajoutez le programme **Bloc-notes** à la liste des applications de confiance. Le fichier exécutable et le processus de l'application de confiance seront toujours soumis à la recherche de virus. Pour exclure entièrement l'application de l'analyse, il faut recourir aux Règles d'exclusion (cf. point 6.3.1, p. 76).

De plus, certaines actions considérées comme dangereuses sont en réalité normales dans le cadre du fonctionnement de divers programmes. Ainsi,

l'interception du texte tapé avec le clavier est une action tout à fait normale pour les programmes de permutation automatique de la disposition du clavier (Punto Switcher, etc.). Afin de tenir compte des particularités de tels programmes et de désactiver le contrôle de leur activité, il est conseillé de les ajouter à la liste des applications de confiance.

De même, l'utilisation d'exclusion d'applications de confiance permet de résoudre divers problèmes de compatibilité entre certaines applications et Kaspersky Internet Security (par exemple, le trafic de réseau en provenance d'un autre ordinateur déjà analysé par un logiciel) et d'accroître les performances de l'ordinateur, ce qui est particulièrement important lors de l'utilisation d'applications serveur.

Par défaut Kaspersky Internet Security analyse les objets ouverts, exécutés et enregistrés par n'importe quel processus logiciel et contrôle l'activité de toutes les activités (programme et réseau) qu'il génère.

La constitution de la liste des applications de confiance s'opère sur l'onglet spécial **Applications de confiance** (cf. ill. 14). Vous pouvez enrichir et modifier la liste à l'aide des boutons **Ajouter**, **Modifier** et **Supprimer** situés à droite.

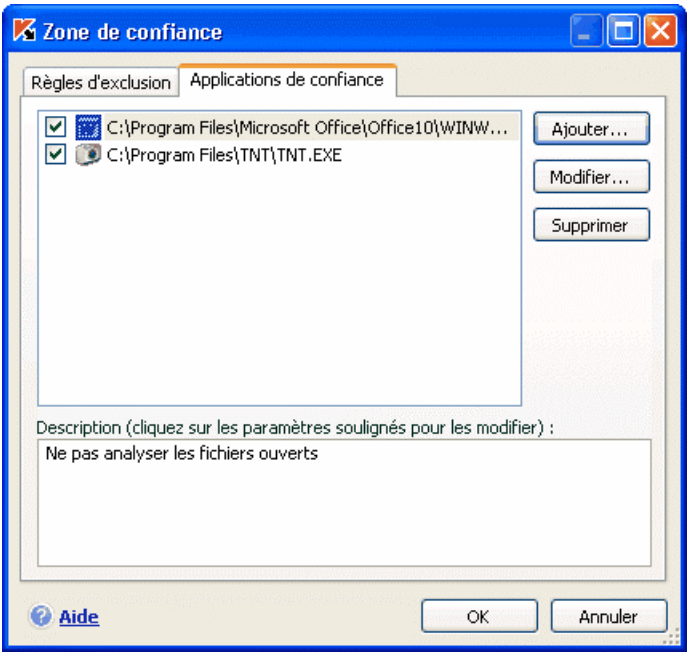


Illustration 14. Liste des applications de confiance

Afin d'ajouter un programme à la liste des applications de confiance :

1. Cliquez sur le bouton **Ajouter** situé dans la partie droite de la fenêtre
2. Dans la fenêtre **Application de confiance** (cf. ill. 15) qui s'ouvre, sélectionnez l'application à l'aide du bouton **Parcourir**. Cette action entraîne l'affichage d'un menu contextuel qui vous permettra au départ du point **Parcourir** de passer à la boîte de dialogue standard de sélection des fichiers et d'indiquer le chemin d'accès au fichier exécutable ou de consulter la liste des applications ouvertes à l'instant au départ du point **Applications** et de sélectionner l'application souhaitée.

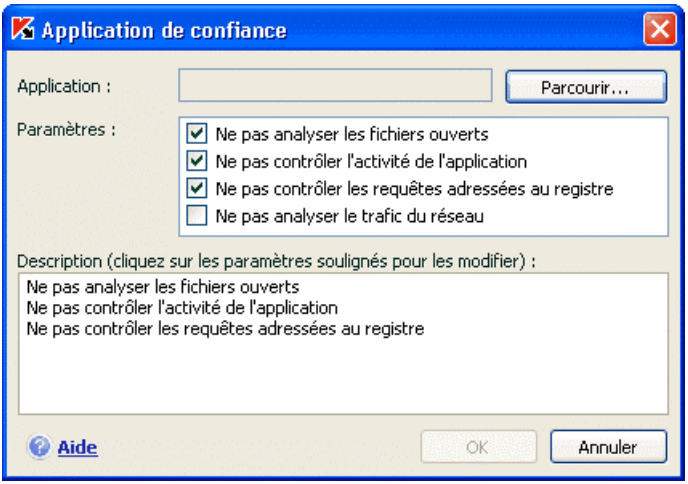


Illustration 15. Ajout d'une application à la liste des applications de confiance

Lors de la sélection du programme Kaspersky Internet Security enregistre les attributs internes du fichier exécutable. Ils serviront à l'identification de l'application pendant l'analyse comme application de confiance.

Le chemin d'accès au fichier est repris automatiquement lors de la sélection du nom. Vous pouvez le modifier manuellement.

Pour le chemin, indiquez le chemin d'accès complet au fichier exécutable ou saisissez le masque *. En cas d'utilisation d'un masque, le processus lancé sera considéré comme processus de confiance quel que soit le répertoire où se trouve le fichier exécutable du programme.

3. Précisez ensuite les processus qui ne seront pas contrôlés par Kaspersky Internet Security:

- **Ne pas analyser les fichiers ouverts** : exclut de l'analyse tous les fichiers ouverts par le processus de l'application de confiance.
- **Ne pas contrôler l'activité de l'application** : exclut de l'analyse dans le cadre de l'utilisation de la défense proactive n'importe quelle activité (y compris les activités suspectes) exécutée par l'application de confiance.
- **Ne pas contrôler les requêtes adressées au registre** : exclut de l'analyse les tentatives de requête adressée à la base de registres système émanant d'une application.
- **Ne pas analyser le trafic du réseau** : exclut de la recherche de virus et de messages non sollicités le trafic de réseau engendré par l'application de confiance. Vous pouvez exclure de l'analyse tout le trafic de réseau de cette application ou limiter l'exclusion à un hôte distant/port en particulier. Pour définir ces restrictions, cliquez sur le lien quelconque qui prend alors la valeur précisez et précisez la valeur de l'hôte distant/du port.

6.4. Lancement d'une tâche de recherche de virus ou de mise à jour avec les privilèges d'un utilisateur

Kaspersky Internet Security 6.0 offre la possibilité de lancer une tâche utilisateur au nom d'un autre utilisateur (représentation). Cette option est désactivée par défaut et les tâches sont exécutées sous le compte de votre enregistrement dans le système.

Par exemple, il se peut que des privilèges d'accès à l'objet à analyser soient requis pour exécuter la tâche. Grâce à ce service, vous pouvez configurer le lancement de la tâche au nom d'un utilisateur qui jouit de tels privilèges.

S'agissant de la mise à jour du logiciel, elle peut être réalisée au départ d'une source à laquelle vous n'avez pas accès (par exemple, le répertoire de mise à jour du réseau) ou pour laquelle vous ne connaissez pas les paramètres d'autorisation du serveur proxy. Vous pouvez utiliser ce service afin de lancer la mise à jour au nom d'un utilisateur qui jouit de ces privilèges.

Pour configurer le lancement d'une tâche au nom d'un autre utilisateur :,

1. Sélectionnez le nom de la tâche dans la section **Analyser (Service)** de la fenêtre principale et grâce au lien Configuration, ouvrez la boîte de dialogue de configuration des paramètres de la tâche.

2. Cliquez sur le bouton **Configuration** dans la boîte de dialogue de configuration de la tâche et passez à l'onglet **Complémentaire** dans la fenêtre qui s'affiche (cf. ill. 16).

Pour activer ce service, cochez la case **Lancer la tâche au nom de l'utilisateur**. Saisissez en dessous les données du compte sous lequel la tâche sera exécutée: nom d'utilisateur et mot de passe.

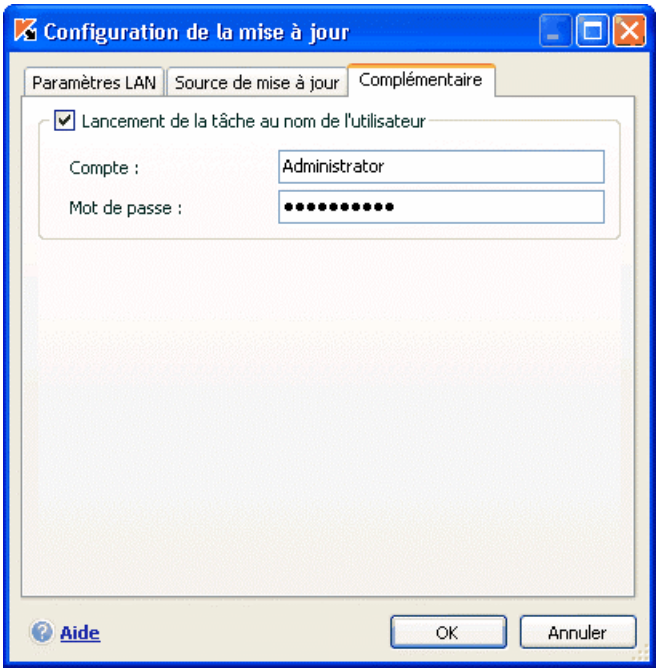


Illustration 16. Configuration du lancement de la mise à jour au nom d'un autre utilisateur

6.5. Programmation du lancement de tâches liées à la recherche de virus et à la mise à jour

Toutes les tâches liées à la recherche de virus ou à la mise à jour peuvent être lancées manuellement ou selon un horaire défini.

S'agissant des tâches liées à la recherche de virus créées lors de l'installation du logiciel, le lancement programmé est désactivé par défaut. La seule exception se

situe au niveau de l'analyse des objets de démarrage qui est réalisée chaque fois que l'ordinateur est allumé. Pour la mise à jour, le lancement programmé est également désactivé. Elle est réalisée automatiquement au fil des diffusions des mises à jour sur les serveurs de Kaspersky Lab.

Si ce mode d'exécution de la tâche ne vous convient pas, il vous suffit de modifier les paramètres du lancement automatique. Pour ce faire, sélectionnez le nom de la tâche dans la section **Analyser** (pour la recherche de virus) ou **Service** (pour la mise à jour) et cliquez sur le lien Configuration afin d'ouvrir la boîte de dialogue de configuration.

Afin d'activer le lancement programmer d'une tâche, cochez la case en regard de la condition de lancement de la tâche dans le bloc **Mode de lancement**. Vous pouvez modifier les conditions de lancement de l'analyse dans la fenêtre **Programmation** (cf. ill. 17) en cliquant sur **Modifier**.

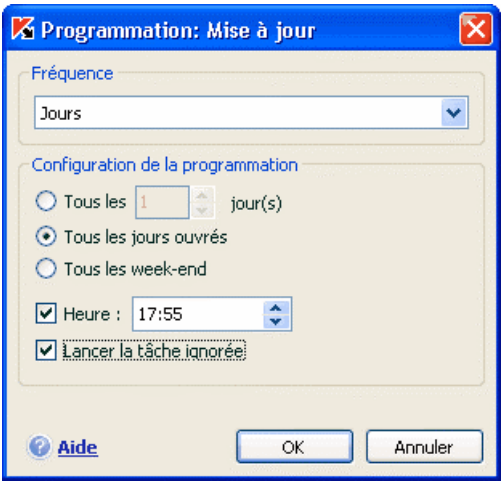


Illustration 17. Programmation de l'exécution de la tâche

L'élément le plus important à définir, c'est la fréquence de lancement. Vous avez le choix entre les options suivantes :

Une fois. La tâche est lancée une fois à l'heure et au jour indiqués.

Minutes. L'intervalle entre les lancements de la tâche se mesure en quelques minutes uniquement. Précisez le nombre de minutes entre chaque lancement dans les paramètres de programmation. L'intervalle maximum est de 59 minutes.

Heures. L'intervalle entre les lancements de la tâche est mesuré en heures. Si vous avez choisi cette fréquence, indiquez l'intervalle dans les paramètres de programmation : **Toutes les X heure(s)** et définissez l'intervalle X. Pour une mise à jour toute les heures, sélectionnez *Toutes les 1 heure(s).*

Jour. Le programme est mis à jour une fois tous les X jours. Dans les paramètres de programmation, définissez la fréquence de lancement de la tâche :

- Sélectionnez **Tous les X jours** et précisez l'intervalle *X* si vous souhaitez qu'un certain nombre de jours s'écoule entre les lancements de la tâche. Ainsi, afin que l'analyse ait lieu un jour sur deux, définissez *Tous les 2 jours*.
- Sélectionnez **Tous les jours ouvrés** si vous souhaitez lancer l'analyse tous les jours du lundi au vendredi.
- Sélectionnez **Tous les week-ends** si vous voulez que la tâche soit lancée uniquement les samedi et dimanche.

  En plus de la fréquence, définissez l'heure à laquelle la tâche sera lancée dans le champ **Heure**.

Semaines. La tâche est lancée certains jours de la semaine. Si vous avez choisi cette fréquence, il vous faudra cocher les jours de lancement de l'analyse dans les paramètres de la programmation. Indiquez également l'heure de lancement de l'analyse dans le champ *Heure*.

Mois. La tâche d'analyse est lancée une fois par mois à l'heure indiquée.

N'oubliez pas que l'analyse des objets de démarrage possède son propre horaire. Vous pouvez configurer le lancement automatique à chaque démarrage de l'ordinateur et/ou après la mise à jour des bases des signatures des menaces. Pour ce faire, cochez les cases adéquates dans la section **Mode de lancement** de la boîte de dialogue de configuration de la tâche.

Si pour une raison quelconque le lancement de la tâche a été ignoré (par exemple, votre ordinateur était éteint à ce moment), vous pouvez configurer le lancement automatique des tâches ignorées dès que cela sera possible. Pour ce faire, cochez la case **Lancer la tâche ignorée** dans la fenêtre de programmation.

6.6. Exportation/importation des paramètres de Kaspersky Internet Security

Kaspersky Internet Security vous permet d'exporter et d'importer les paramètres de fonctionnement.

Cela est utile si vous avez installé le logiciel sur un ordinateur chez vous et au bureau. Vous pouvez configurer le logiciel selon un mode qui vous convient pour

le travail à domicile, conserver ces paramètres sur le disque et à l'aide de la fonction d'importation, les importer rapidement sur votre ordinateur au travail. Les paramètres sont enregistrés dans un fichier de configuration spécial.

Pour exporter les paramètres actuels de fonctionnement du logiciel :

1. Ouvrez la fenêtre principale de Kaspersky Internet Security.
2. Cliquez sur le lien **Configuration** dans la section **Protection**.
3. Cliquez sur le bouton **Exporter** dans le bloc **Profil de configuration.**
4. Saisissez le nom du fichier de configuration et précisez l'emplacement de la sauvegarde.

Pour importer les paramètres du fichier de configuration :

1. Ouvrez la fenêtre principale de Kaspersky Internet Security.
2. Cliquez sur le lien **Configuration** dans la section **Protection**.
3. Cliquez sur **Importer** et sélectionnez le fichier contenant les paramètres que vous souhaitez importer dans Kaspersky Internet Security.

6.7. Restauration des paramètres par défaut

Vous pouvez toujours revenir aux paramètres recommandés du logiciel. Ces paramètres sont les paramètres optimaux recommandés par les experts de Kaspersky Lab. La restauration s'opère à l'aide de l'Assistant de configuration initiale du logiciel.

Pour restaurer les paramètres de protection :

1. Sélectionnez la section **Protection** et ouvrez la fenêtre des paramètres du logiciel à l'aide du lien Configuration.
2. Cliquez sur le bouton **Par défaut** dans la section **Profil de configuration**.

Dans la fenêtre qui s'affiche, vous aurez la possibilité de définir les paramètres et de quels composants que vous souhaitez conserver en plus de la restauration du niveau de protection recommandé.

La liste propose les composants du logiciel dont les paramètres ont été modifiés par l'utilisateur ou assimilés par le logiciel durant l'entraînement (Anti-Hacker et Anti-Spam). Si des paramètres uniques ont été définis pour un composant quelconque, ils figureront également dans la liste.

Ces paramètres uniques sont : des règles d'exclusion prédifinies pour une auto-protection des composants du programme, les listes des adresses mails de confiances et les règles d'application de la Défense Proactive.

Parmi les paramètres que vous pouvez conserver, il y a les listes "blanche" et "noire" des expressions et des adresses utilisées par Anti-Spam, la liste des adresses Internet et des numéros d'accès de confiance utilisée par l'antivirus Internet et Anti-Escroc, les règles d'exclusion pour les composants du programme, les règles de filtrage des paquets et les règles des applications d'Anti-Hacker ainsi que les règles pour les applications de la défense proactive.

Les règles d'exclusions composées pour les composants du logiciel, les listes d'adresse de confiance utilisées par l'antivirus Internet et les règles pour les applications de la défense proactives figurent parmi ces paramètres uniques

Ces listes sont composées lors de l'utilisation du logiciel, sur la base de tâches individuelles et des exigences de sécurité. Cette opération requiert beaucoup de temps. Pour cette raison, nous vous conseillons de conserver ces paramètres lors de la restauration de la configuration initiale du programme.

Par défaut, tous les paramètres uniques présentés dans la liste seront conservés (la case correspondante n'est pas sélectionnée). Si certains paramètres n'ont pas besoin d'être conservés, cochez la case située en regard de ceux-ci.

Une fois la configuration terminée, cliquez sur **Suivant**. Cela lancera l'Assistant de configuration initiale du logiciel (cf. point 3.2, p. 37). Suivez les instructions affichées.

Lorsque vous aurez quitté l'Assistant, tous les composants de la protection fonctionneront selon le niveau **Recommandé** et tiendront compte des paramètres que vous avez décidé de conserver lors de la restauration. De plus, les paramètres définis à l'aide de l'Assistant seront appliqués.

CHAPITRE 7. PROTECTION ANTIVIRUS DU SYSTEME DE FICHIERS DE L'ORDINATEUR

Kaspersky Internet Security contient un composant spécial qui permet d'éviter l'infection du système de fichiers de votre ordinateur. Il s'agit de *l'antivirus de fichiers*. Il est lancé en même temps que le système d'exploitation, demeure en permanence dans la mémoire vive de l'ordinateur et analyse tous les programmes ou fichiers que vous ouvrez, enregistrez ou exécutez.

L'icône de Kaspersky Internet Security dans la barre des tâches indique le fonctionnement du composant. Cette icône prend cette apparence  chaque fois qu'un fichier est analysé.

Par défaut, l'antivirus de fichiers analyse uniquement les NOUVEAUX fichiers ou les fichiers MODIFIES, c'est-à-dire les fichiers dans lesquels des données ont été ajoutées ou modifiées depuis la dernière requête. Et cela, grâce aux nouvelles technologies iChecker™ et iSwift™. Cette technologie repose sur l'utilisation d'un tableau des sommes de contrôle des fichiers. L'analyse des fichiers est réalisée selon l'algorithme suivant :

1. Tout fichier qui reçoit une requête de l'utilisateur ou d'un programme quelconque est intercepté par le composant.
2. L'antivirus de fichiers vérifie si la base iChecker ou iSwift contient des informations relatives au fichier intercepté. Ensuite, le processus peut suivre l'une des deux voies suivantes :
    - Si la base ne contient aucune information relative à ce fichier, celui-ci sera soumis à une analyse antivirus détaillée. La somme de contrôle est vérifiée et le fichier traité est enregistré dans la base.
    - Si la base contient des informations relatives au fichier, l'antivirus de fichiers compare l'état actuel du fichier à celui enregistré dans la base au moment de la dernière analyse. En cas d'équivalence parfaite, le fichier est transmis à l'utilisateur sans analyse. Si le fichier diffère d'une manière ou d'une autre, il est soumis à une analyse en profondeur et les nouvelles informations à son sujet sont enregistrées dans la base.

Le processus d'analyse contient les étapes suivantes :

1. Le fichier est soumis à la recherche d'éventuels virus. L'identification des objets malveillants s'opère sur la base des *signatures des menaces* utilisées par le composant. Les signatures contiennent la définition de tous les programmes malveillants, menaces et attaques de réseau connus à ce jour et leur mode d'infection.
2. Les comportements suivants sont possibles en fonction des résultats de l'analyse :
    a. Si le fichier contient un code malveillant, l'antivirus de fichiers le bloque, place une copie dans le *dossier de sauvegarde* et tente de le neutraliser. Si la réparation réussit, l'utilisateur peut utiliser le fichier. Dans le cas contraire, le fichier est supprimé.
    b. Si le fichier contient un code semblable à un code malveillant et que ce verdict ne peut pas être garanti à 100%, le fichier est placé en *quarantaine*.
    c. Si aucun code malveillant n'a été découvert dans le fichier, le destinataire pourra l'utiliser immédiatement.

7.1. Sélection du niveau de protection des fichiers

L'antivirus de fichiers protège les fichiers que vous utilisez selon un des niveaux suivants (cf. ill. 18):

Elevé : le contrôle des fichiers ouverts, enregistrés et modifiés est total.

Recommandé : les paramètres de ce niveau correspondent aux paramètres recommandés par les experts de Kaspersky Lab. Ils prévoient l'analyse des objets suivants :

- Programmes et objets en fonction du contenu;
- Uniquement les nouveaux objets et les objets modifiés depuis la dernière analyse;
- Les archives dont la taille ne dépasse pas 8Mo;
- Les fichiers d'installation; les objets OLE intégrés.

- **Faible** : ce niveau vous permet de travailler sans problèmes avec les applications gourmandes en mémoire vive car le volume de fichiers analysés est réduit.

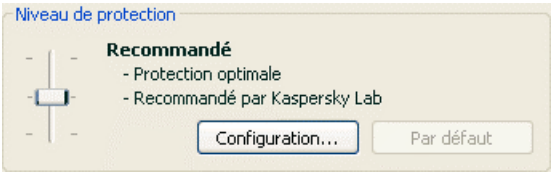


Illustration 18. Niveau de protection d'Antivirus Fichiers

Par défaut, la protection des fichiers s'opère selon les paramètres du niveau **Recommandé**.

Vous pouvez augmenter ou réduire le niveau de protection des fichiers en sélectionnant un autre niveau ou en modifiant les paramètres du niveau actuel.

Pour modifier le niveau de protection :

Déplacez simplement le curseur. Ce faisant, vous modifiez le rapport entre la vitesse de l'analyse et la quantité d'objets analysés : plus le nombre de fichiers soumis à l'analyse sera réduit, plus la vitesse de l'analyse sera élevée

Si aucun des niveaux prédéfinis ne répond à vos attentes, vous pouvez procéder à une configuration complémentaire des paramètres de la protection. Dans ce cas, il est conseillé de choisir le niveau le plus proche de vos besoins en guise de point de départ et d'en modifier les paramètres. Dans ce cas, le niveau devient **Utilisateur**. Voici un exemple d'une situation où le niveau Utilisateur serait le plus indiqué pour la protection des fichiers.

Exemple:

Dans le cadre de votre activité, vous travaillez avec de nombreux fichiers de divers formats et notamment des fichiers assez volumineux. Vous ne voulez pas prendre de risque en excluant de l'analyse certains fichiers sur la base de leur extension ou de leur taille, même si une telle décision va avoir des répercussions sur les performances de votre ordinateur.

Conseil pour la sélection du niveau :

Sur la base de ces informations, nous pouvons dire que le risque d'infection par un programme malveillant est relativement élevé. La taille et le type de fichiers utilisés sont trop hétérogènes et les exclure de l'analyse exposerait les informations sauvegardées sur l'ordinateur à des risques. Ce qui compte ici, c'est l'analyse des fichiers utilisés au niveau du contenu et non pas de leur extension.

Dans ce cas, il est conseillé d'utiliser le niveau **Recommandé** qui sera modifié de la manière suivante : lever les restrictions sur la taille des fichiers analysés et optimiser le fonctionnement de l'antivirus de fichiers en analysant uniquement les nouveaux fichiers et les fichiers modifiés.

Cela permettra de réduire la charge de l'ordinateur pendant l'analyse des fichiers et de continuer à travailler sans problème avec d'autres applications.

Pour modifier les paramètres du niveau de protection actuel :

cliquez sur **Configuration** dans la fenêtre des paramètres de l'antivirus de fichiers, modifiez les paramètres selon vos besoins et cliquez sur **OK**.

Un quatrième niveau de protection est ainsi configuré : **Utilisateur** selon les paramètres que vous aurez définis.

7.2. Configuration de la protection des fichiers

La protection des fichiers sur l'ordinateur est définie par un ensemble de paramètres. Ils peuvent être scindés selon les groupes suivants :

- Les paramètres qui définissent les types de fichiers soumis à l'analyse antivirus (cf. point 7.2.1, p. 93);
- Les paramètres qui définissent la zone protégée (cf. point 7.2.2, p. 96);
- Les paramètres qui définissent les actions à réaliser sur l'objet dangereux (cf. point 7.2.4, p. 98).;

Tous ces paramètres sont abordés en détails ci-après.

7.2.1. Définition du type de fichiers analysés

La définition du type de fichiers analysés vous permet de déterminer le format des fichiers qui seront soumis à l'analyse antivirus à l'ouverture, l'exécution et l'enregistrement, ainsi que leur taille et le disque sur lequel ils sont enregistrés.

Afin de simplifier la configuration, tous les fichiers ont été séparés en deux groupes : *simples* et *composés.* Les fichiers simples ne contiennent aucun objet. (par exemple, un fichier texte). Les fichiers composés peuvent contenir plusieurs objets et chacun de ceux-ci peut à son tour contenir plusieurs pièces jointes. Les exemples ne manquent pas : archives, fichiers contenant des macros, des tableaux, des messages avec des pièces jointes, etc.

Le type de fichiers à analyser est défini dans la section **Types de fichiers** (cf. ill. 19). Choisissez l'une des trois options :

- **Analyser tous les fichiers.** Dans ce cas, tous les objets ouverts, exécutés et enregistrés dans le système de fichiers seront analysés sans exception.
- **Analyser les programmes et les documents (selon le contenu).** L'antivirus de fichiers analysera uniquement les fichiers qui présentent un risque d'infection, c.-à-d. les fichiers dans lesquels un virus pourrait s'insérer.

  Informations.

  Il existe des fichiers dans lesquels aucun virus ne peut s'incruster car le code du fichier ne contient aucun point d'accrochage pour le virus. Les fichiers texte en sont un exemple.

  Avant de passer à la recherche de virus dans le fichier, le système définit le format du fichier (txt, doc, exe, etc.) en analysant l'en-tête interne du fichier. Si l'analyse détermine qu'aucun des fichiers de ce format ne peut être infecté, le fichier n'est pas soumis à l'analyse et devient tout de suite accessible. Si le format du fichier laisse supposer un risque d'infection, le fichier est soumis à l'analyse.

- **Analyser les programmes et les documents (selon l'extension)**. Dans ce cas, l'antivirus de fichiers analyse uniquement les fichiers potentiellement infectés et le format du fichier est pris en compte sur la base de son extension. En cliquant sur le lien extension, vous pourrez découvrir la liste des extensions des fichiers (cf. point A.1, p. 290) qui seront soumis à l'analyse dans ce cas.

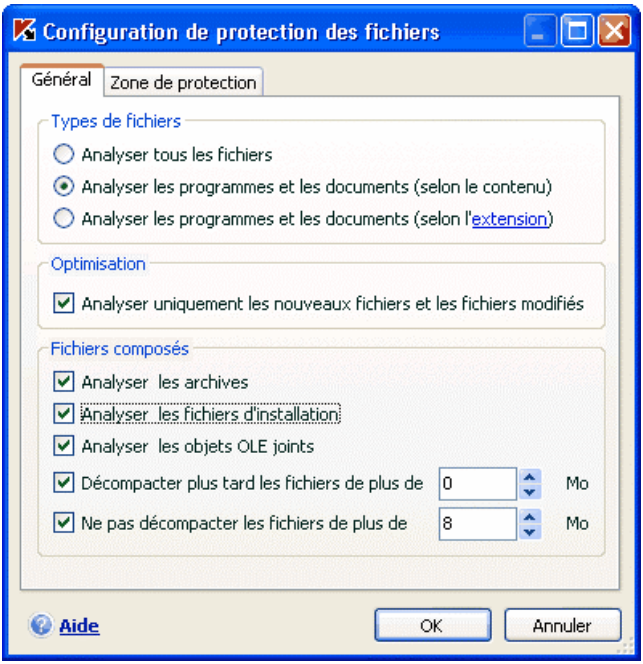


Illustration 19. Sélection du type de fichier soumis à l'analyse antivirus

Conseil.

Il ne faut pas oublier qu'une personne mal intentionnée peut envoyer un virus sur votre ordinateur dans un fichier dont l'extension est txt alors qu'il s'agit en fait d'un fichier exécutable renommer en fichier txt. Si vous sélectionnez l'option **Analyser les programmes et les documents (selon l'extension)**, ce fichier sera ignoré pendant l'analyse. Si vous sélectionnez l'option **Analyser les programmes et les documents (selon le contenu)**, l'antivirus de fichiers ignorera l'extension, analysera l'en-tête du fichier et découvrira qu'il s'agit d'un fichier exe. Le fichier sera alors soumis à une analyse antivirus minutieuse.

Vous pouvez, dans la section **Optimisation**, préciser que seuls les nouveaux fichiers et ceux qui ont été modifiés depuis la dernière analyse seront soumis à l'analyse antivirus. Ce mode réduit considérablement la durée de l'analyse et augmente la vitesse de traitement du logiciel. Pour ce faire, il est indispensable de cocher la case ☑ **Analyser uniquement les nouveaux fichiers et les fichiers modifiés**. Ce mode de travail touchera aussi bien les fichiers simples que les fichiers composés.

Indiquez, dans la section **Fichiers composés**, les types de fichiers composés qui devront être soumis à l'analyse antivirus :

- **Analyser toutes les archives/uniquement les nouvelles archives** : analyse les archives au format ZIP, CAB, RAR, ARJ, y compris les archives protégées par un mot de passe.
- **Analyser tous les/uniquement les nouveaux fichiers d'installation** : recherche la présence d'éventuels virus dans les archives autoextractibles.
- **Analyser tous les/uniquement les nouveaux objets OLE joints** : analyse les objets intégrés au fichier (exemple : tableau Excel, macro dans un document Word, pièce jointe d'un message électronique, etc.)

Pour chaque type de fichier composé, vous pouvez décider d'analyser tous les fichiers ou uniquement les nouveaux. Pour ce faire, cliquez sur le lien situé en regard du nom de l'objet. Il change de valeur lorsque vous appuyez sur le bouton gauche de la souris. Si vous avez défini dans la section **Optimisation** l'analyse uniquement des nouveaux fichiers et des fichiers modifiés, il sera impossible de sélectionner un type de fichier composé.

Afin de préciser le type de fichiers composés qu'il ne faut pas analyser, utilisez l'un des paramètres suivants :

- **Décompacter plus tard les fichiers de plus de ... Mo**. Lorsque la taille de l'objet composé dépasse cette limite, il sera analysé en tant qu'objet unique (l'en-tête est analysée) et il pourra être manipulé par l'utilisateur. L'analyse des objets qu'il contient sera réalisée plus tard. Si la case n'est pas cochée, l'accès aux fichiers dont la taille est supérieure à la valeur définie sera bloqué jusque la fin de l'analyse des objets.
- **Ne pas décompacter les fichiers de plus de … Mo**. Dans ce cas, le fichier dont la taille est supérieure à la valeur indiquée sera ignoré par l'analyse.

7.2.2. Constitution de la zone protégée

Par défaut, l'antivirus de fichiers analyse tous les fichiers dès qu'une requête leur est adressée, quel que soit le support sur lequel ils se trouvent (disque dur, cédérom ou carte Flash).

Vous pouvez définir la zone protégée. Pour ce faire :

1. Sélectionnez **Antivirus Fichiers** dans la fenêtre principale et ouvrez la boîte de dialogue de configuration du composant en cliquant sur le lien Configuration
2. Cliquez sur le bouton **Configuration** et sélectionnez l'onglet **Zone de protection** dans la fenêtre qui s'ouvre (cf. ill. 20).

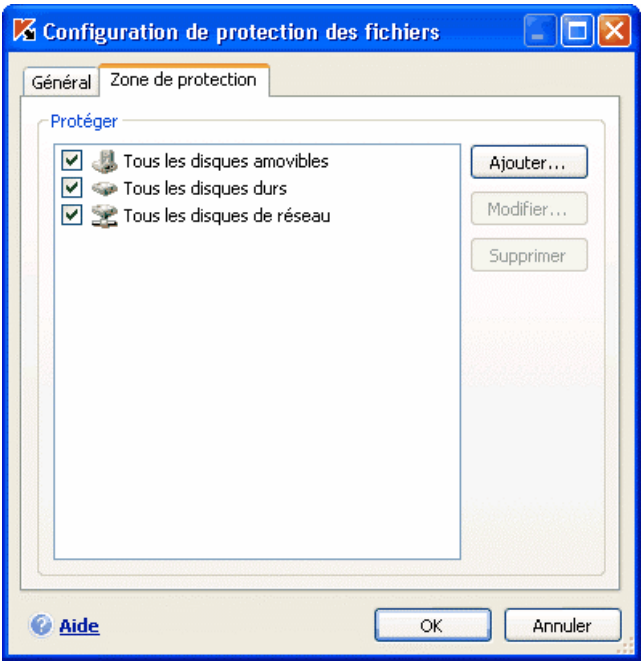


Illustration 20. Constitution de la zone protégée

L'onglet reprend la liste des objets qui seront soumis à l'analyse de l'antivirus de fichiers. La protection de tous les objets situés sur les disques durs, les disques amovibles et les disques de réseaux connectés à votre ordinateur est activée par défaut. Vous pouvez enrichir et modifier cette liste à l'aide des boutons **Ajouter**, **Modifier** et **Supprimer**.

Si vous souhaitez restreindre le nombre d'objets protégés, vous pouvez suivre l'une des méthodes suivantes :

- Indiquer uniquement les répertoires, disques ou fichiers qui doivent être protégés.
- Constituer une liste des objets qui ne doivent pas être protégés.
- Utiliser simultanément la première et la deuxième méthode, c.-à-d. définir une zone de protection de laquelle une série d'objets seront exclus.

Attention.

N'oubliez pas que l'antivirus de fichiers recherchera la présence éventuelle de virus uniquement dans les fichiers inclus dans la zone de protection. Les fichiers qui ne font pas partie de cette zone seront accessibles sans analyse. Cela augmente le risque d'infection de votre ordinateur !

7.2.3. Restauration des paramètres de protection des fichiers par défaut

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

Pour restaurer les paramètres de protection des fichiers par défaut :

1. Sélectionnez **Antivirus Fichiers** dans la fenêtre principale et ouvrez la boîte de dialogue de configuration du composant en cliquant sur le lien Configuration
2. Cliquez sur le bouton **Par défaut** dans le bloc **Niveau de protection.**

7.2.4. Sélection de l'action exécutée sur les objets

Si l'analyse d'un fichier détermine une infection ou une possibilité d'infection, la suite du fonctionnement de l'antivirus de fichiers dépendra de l'état de l'objet et de l'action sélectionnée.

L'antivirus de fichier peut attribuer l'un des statuts suivants à l'objet :

- Etat de l'un des programmes malveillants (exemple, *virus, cheval de Troie*) (cf. point 1.2, p. 11).
- *Potentiellement infecté* lorsqu'il n'est pas possible d'affirmer avec certitude si l'objet est infecté ou non. Cela signifie que le code du fichier contient une séquence semblable à celle d'un virus connu mais modifié ou qui évoque, par sa structure, la séquence d'un virus.

Par défaut, tous les objets infectés sont réparés et tous les objets potentiellement infectés sont placés en quarantaine.

Pour modifier l'action à exécuter sur l'objet :

Sélectionnez **Antivirus Fichiers** dans la fenêtre principale et ouvrez la boîte de dialogue de configuration du composant en cliquant sur le lien Configuration Toutes les actions possibles sont reprises dans la section correspondante (cf. ill. 21).

Illustration 21. Actions que peut exécuter Antivirus Fichiers sur un objet dangereux

Si vous avez choisi l'action	En cas de découverte d'un objet dangereux
Confirmer l'action	L'antivirus de fichiers affiche un message d'avertissement qui reprend les informations relatives à l'objet malveillant source de l'infection (potentielle) et propose l'une des actions suivantes. Les actions varient en fonction de l'état de l'objet.
Bloquer l'accès	L'antivirus de fichiers bloque l'accès à l'objet. Les informations sont consignées dans le rapport (cf. point 16.3, p. 237). Vous pouvez plus tard tenter de réparer cet objet.
Bloquer l'accès **Réparer**	L'antivirus de fichiers bloque l'accès à l'objet et tente de le réparer. Si la réparation réussit, l'objet est à nouveau disponible. Si la réparation échoue, l'objet est placé en quarantaine (cf. point 16.1, p. 231). Les informations relatives à cette situation sont consignées dans le rapport. Il est possible de tenter de réparer cet objet ultérieurement.
Bloquer l'accès **Réparer**	L'antivirus de fichiers bloque l'accès à l'objet et tente de le réparer. Si la réparation réussit, l'objet est à

Si vous avez choisi l'action	En cas de découverte d'un objet dangereux
☑ **Supprimer si la réparation n'est pas possible**	réparation réussit, l'objet est à nouveau disponible. Si la réparation de l'objet échoue, il sera supprimé. Une copie de sauvegarde sera conservée dans le dossier de sauvegarde (cf. point 16.2, p. 235).
◉ **Bloquer l'accès** ☑ **Réparer** ☑ **Supprimer**	L'antivirus de fichiers bloque l'accès à l'objet et le supprime.

Quel que soit le statut de l'objet (infecté ou potentiellement infecté), Kaspersky Internet Security crée une copie de sauvegarde avant de tenter de le réparer ou de le supprimer. Cette copie est placée dans le dossier de sauvegarde au cas où il faudrait restaurer l'objet ou si la réparation devenait possible.

7.3. Réparation différée des objets

Si vous avez sélectionné ◉ **Bloquer l'action** en tant qu'action réalisée sur les objets malveillants, ces objets ne seront pas réparés et ils ne seront pas accessibles.

Si vous avez sélectionné

◉ **Bloquer l'accès**

☑ **Réparer**

alors, tous les objets qui n'ont pas été réparés seront bloqués.

Pour pouvoir à nouveau accéder aux objets bloqués, vous devrez les réparer. Pour ce faire :

1. Sélectionnez **Antivirus Fichiers** dans la fenêtre principale du logiciel et cliquez avec le bouton gauche de la souris n'importe où dans le bloc Statistiques.
2. Sélectionnez les objets qui vous intéressent sur l'onglet **Infectés** et cliquez sur **Actions** ⟶ **Réparer tous**.

Si la réparation a réussi, vous pourrez à nouveau travailler avec cet objet. S'il est impossible de le réparer vous pourrez choisir entre *supprimer* ou *ignorer*. Dans ce dernier cas, l'accès au fichier sera autorisé. Cela augmente toutefois le risque d'infection de votre ordinateur ! Il est vivement conseillé de ne pas ignorer les objets malveillants.

CHAPITRE 8. PROTECTION ANTIVIRUS DU COURRIER

Kaspersky Internet Security contient un composant spécial qui protège le courrier entrant et sortant. Il s'agit de *l'antivirus de messagerie électronique.* Il est lancé au démarrage du système d'exploitation, se trouve en permanence dans la mémoire système de l'ordinateur et analyse tous les messages envoyés et reçus via les protocoles POP3, SMTP, IMAP, MAPI[1] et NNTP.

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

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

1. Chaque message envoyé ou reçu par l'utilisateur est intercepté par l'antivirus de messagerie électronique.
2. Le message est décomposé selon ses parties constitutives, à savoir : l'en-tête du message, le corps du message et la pièce jointe.
3. Le corps et la pièce jointe (y compris les objets OLE) sont soumis à la recherche d'éventuels objets dangereux. L'identification des objets malveillants est réalisée à l'aide des *signatures de menaces* utilisées par le logiciel et d'un algorithme heuristique. Les signatures contiennent la définition de tous les programmes malveillants connus à ce jour et de leur mode d'infection. L'algorithme heuristique permet d'identifier les nouveaux virus dont les définitions ne sont pas encore reprises dans les signatures de menaces.
4. Les comportements suivants sont envisageables à l'issue de l'analyse :
    - Si le corps du message ou la pièce jointe contient un code malveillant, l'antivirus de messagerie électronique bloque le message, place une copie de l'objet infecté dans le *dossier de sauvegarde* et tente de réparer l'objet. Si la réparation réussit, l'utilisateur peut accéder au message. Dans le cas contraire, l'objet infecté est supprimé du message. Suite au traitement antivirus, un texte spécial est inclus dans l'objet du message.

[1] L'analyse du courrier sur le protocole MAPI est réalisé à l'aide d'un plug-in spécial pour Microsoft Office Outlook et The Bat !

Ce texte indique que le message a été traité par Kaspersky Internet Security.

- Si le corps du message ou la pièce jointe contient un code semblable à un code malveillant, sans garantie, la partie suspecte du message est placée dans un dossier spécial : la *quarantaine*.
- Si aucun code malveillant n'a été découvert dans le message, le destinataire pourra y accéder immédiatement.

Un plug-in spécial (cf. point 8.2.2, p. 106) qui permet de réaliser une configuration plus fine de l'analyse du courrier a été ajouté à Microsoft Outlook.

Si vous utilisez The Bat!, Kaspersky Internet Security peut être utilisé conjointement à d'autres logiciels antivirus. Dans ce cas, les règles de traitement du courrier (cf. point 8.2.3, p. 108) sont définies directement dans The Bat! et prévalent sur les paramètres de protection du courrier de Kaspersky Internet Security.

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

Sous Thunderbird, les messages transmis via le protocole IMAP ne sont pas soumis à l'analyse antivirus en cas d'utilisation de règles de tri des messages.

Il convient de noter que les messages électroniques transmis via le protocole SSL ne sont pas analysés par l'antivirus de messagerie électronique.

8.1. Sélection du niveau de protection du courrier

Kaspersky Internet Security assure la protection du courrier selon un des 3 niveaux suivants (cf. ill. 22):

Elevé : le contrôle du courrier entrant et sortant est total. Le logiciel analyse en détail les pièces jointes, indépendamment du temps d'analyse, y compris les archives.

Recommandé : les paramètres de ce niveau correspondent aux paramètres recommandés par les experts de Kaspersky Lab. L'analyse porte sur les mêmes objets que ceux du niveau **Elevé**, à l'exclusion des pièces jointes et des messages dont l'analyse dure plus de trois minutes.

Faible : la configuration de ce niveau de protection vous permet de travailler sans problèmes avec les applications gourmandes en mémoire vive car le volume de messages analysés est réduit. Ce niveau assure uniquement l'analyse du courrier entrant, mais pas des archives et des objets (messages) joints dont l'analyse dure plus de trois minutes. L'utilisation de ce niveau est recommandée uniquement si d'autres moyens de protection du courrier sont installés sur votre ordinateur.

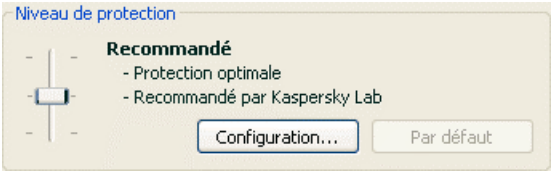


Illustration 22. Sélection du niveau de protection du courrier

Par défaut, la protection du courrier s'opère selon les paramètres du niveau **Recommandé**.

Vous pouvez augmenter ou réduire le niveau de protection du courrier en sélectionnant un autre niveau ou en modifiant les paramètres du niveau actuel.

Pour modifier le niveau de protection :

Déplacez simplement le curseur. Ce faisant, vous modifiez le rapport entre la vitesse de l'analyse et la quantité d'objets analysés : plus le nombre d'objets de messages électroniques soumis à l'analyse sera réduit, plus la vitesse de l'analyse sera élevée

Si l'un des niveaux proposés par défaut ne convient pas à vos exigences, vous pouvez modifier les paramètres. Dans ce cas, le niveau devient **Utilisateur**. Voici un exemple d'une situation où le niveau Utilisateur serait le plus indiqué pour la protection du courrier.

Exemple:

votre ordinateur est en dehors du réseau local et se connecte à Internet via un modem. Vous utilisez Microsoft Outlook Express pour envoyer et recevoir vos messages ainsi qu'un service de messagerie en ligne gratuit. Pour diverses raisons, votre courrier contient souvent des archives en pièce jointe. Comment protéger au maximum votre ordinateur contre une infection via le courrier électronique ?

Conseil pour la sélection du niveau :

l'analyse de la situation permet de conclure que le risque d'infection via le courrier électronique est très élevé (absence de protection centralisée du courrier et des moyens d'accès à Internet).

Dans ce cas, il est conseillé d'utiliser le niveau **Elevé** qui sera modifié de la manière suivante : il est conseillé de réduire la durée d'analyse des objets en pièce jointe, par exemple 1 à 2 minutes. La majorité des archives jointes sera analysée et la vitesse de traitement du courrier ne sera pas sensiblement ralentie.

Pour modifier les paramètres du niveau de protection proposé par défaut :

cliquez sur **Configuration** dans la fenêtre des paramètres de l'antivirus de messagerie électronique, modifiez les paramètres selon vos besoins et cliquez sur **OK**.

8.2. Configuration de la protection du courrier

Les règles d'analyse du courrier sont définies à l'aide de paramètres. Ils peuvent être scindés selon les groupes suivants :

- Les paramètres qui définissent le flux de messagerie protégé (cf. point 8.2.1, p. 104);
- Les paramètres qui définissent l'analyse des messages dans Microsoft Office Outlook (cf. point 8.2.2, p. 106) et The Bat! (cf. point 8.2.3, p. 108).;
- Les paramètres qui définissent les actions à réaliser sur les objets dangereux des messages (cf. point 8.2.5, p. 110).

Tous ces types de paramètres sont abordés en détails ci-après.

8.2.1. Sélection du flux de messagerie protégé

L'antivirus de messagerie vous permet de choisir quel flux de messages électroniques sera soumis à la recherche d'éventuels objets dangereux.

Par défaut, le composant assure la protection du courrier selon le niveau **Recommandé**. Cela signifie que le courrier entrant et le courrier sortant sont analysés. Au tout début de l'utilisation, il est conseillé d'analyser le courrier sortant car il est possible que votre ordinateur abrite des vers de messagerie qui se propagent via le courrier électronique. Cela permet d'éviter les inconvénients liés à la diffusion non contrôlée de messages infectés depuis votre ordinateur.

Si vous êtes certains que les messages que vous envoyez ne contiennent pas d'objets dangereux, vous pouvez désactiver la protection du courrier sortant. Pour ce faire :

1. Cliquez sur **Configuration** dans la fenêtre des paramètres de l'antivirus de messagerie électronique.
2. Dans la fenêtre de configuration de l'antivirus de messagerie électronique (cf. ill.), sélectionnez l'onglet **Général** et choisissez l'option **Uniquement le courrier entrant** dans le bloc **Zone d'analyse**.

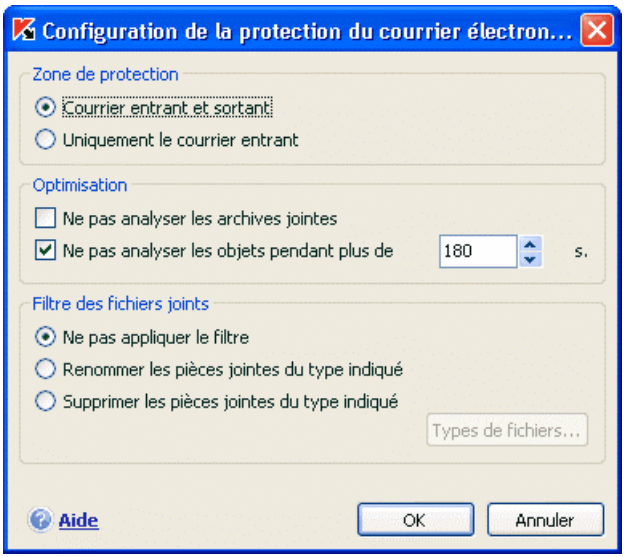


Illustration 23. Configuration de la protection du trafic de messagerie

En plus de la sélection du flux de messagerie, vous pouvez également préciser s'il faut contrôler les archives en pièce jointe et définir la durée maximale d'analyse d'un objet. Ces paramètres sont définis dans le bloc **Optimisation**.

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

Si vous travaillez dans un environnement protégé, vous pouvez modifier la limite de la durée d'analyse des objets afin d'accroître la vitesse.

Dans le bloc **Filtre des fichiers joints**, vous pouvez configurer les conditions de filtrage des objets joints aux messages électroniques :

- **Ne pas appliquer le filtre** : ne procède pas au filtrage complémentaire des pièces jointes.
- **Renommer les pièces jointes du type indiqué** : filtre les pièces jointes d'un certain format et remplace le dernier caractère du nom du fichier

par un trait de soulignement. Vous pouvez sélectionner le type de fichier dans la fenêtre qui s'ouvre à l'aide du bouton **Types de fichiers**.

Supprimer les pièces jointes du type indiqué : filtre et supprime les fichiers en pièce jointe d'un certain type. Vous pouvez sélectionner le type de fichier dans la fenêtre qui s'ouvre à l'aide du bouton **Types de fichiers**.

Pour obtenir de plus amples informations sur les types de fichier qui peuvent être filtrés, consultez la rubrique A.1 à la page 290.

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

8.2.2. Configuration de l'analyse dans Microsoft Office Outlook

Si vous utilisez Microsoft Outlook, vous pouvez configurer davantage la recherche d'éventuels virus dans votre courrier.

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

Le plug-in prend la forme de l'onglet **Antivirus Courrier** dans le menu **Services** → **Paramètres**(cf. ill. 24).

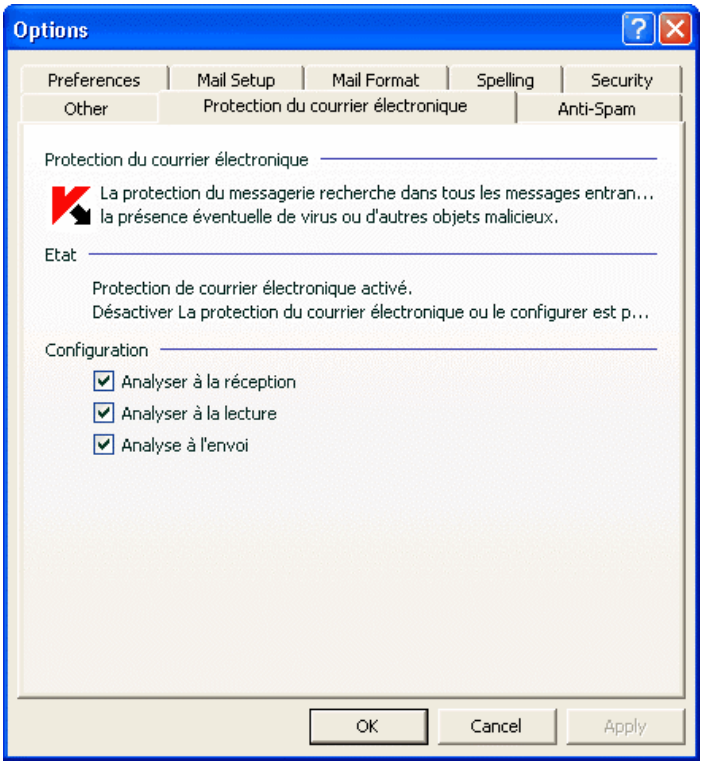


Illustration 24. Configuration détaillée de la protection du courrier dans Microsoft Office Outlook

Sélectionnez un mode d'analyse du courrier :

- **Analyser à la réception** : analyse chaque message dès son arrivée dans votre boîte aux lettres.
- **Analyser à la lecture** : analyse le message lorsque vous l'ouvrez pour le lire.
- **Analyser à l'envoi** :analyse tous les messages que vous envoyez, au moment de l'envoi.

Attention !

Si Microsoft Outlook se connecte au serveur de messagerie via le protocole IMAP, il est conseillé de ne pas utiliser le mode **Analyser à la réception.** Ce mode implique la copie du message sur l'ordinateur local au moment de l'arrivée sur le serveur, ce qui supprimera l'avantage du protocole IMAP, à savoir l'économie de trafic et la gestion des lettres non sollicitées sur le serveur sans les copier sur l'ordinateur de l'utilisateur.

L'action qui sera exécutée sur l'objet dangereux du message est définie dans les paramètres de l'antivirus de messagerie électronique. Pour passer à la configuration de ces paramètres, cliquez sur ici.

8.2.3. Configuration de l'analyse du courrier dans The Bat!

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

Attention !

Les paramètres de l'antivirus de messagerie qui définissent l'analyse ou non du courrier entrant et sortant ainsi que les actions à réaliser sur les objets dangereux de messages et les exclusions sont ignorées. Les seuls élément pris en considération par The Bat!, sont l'analyse des pièces jointes et la restriction sur la durée de l'analyse d'un objet du message (cf. point 8.2.1, p. 104).

Pour passer à la configuration de la protection du courrier indésirable dans The Bat! :

1. Sélectionnez l'élément **Configuration** dans le menu **Propriétés** du client de messagerie.
2. Sélectionnez le nœud **Protection contre les virus** dans l'arborescence des paramètres.

Les paramètres de protection contre le courrier indésirable (cf. ill. 25) sont appliqués à tous les modules antivirus de l'ordinateur compatibles avec The Bat!

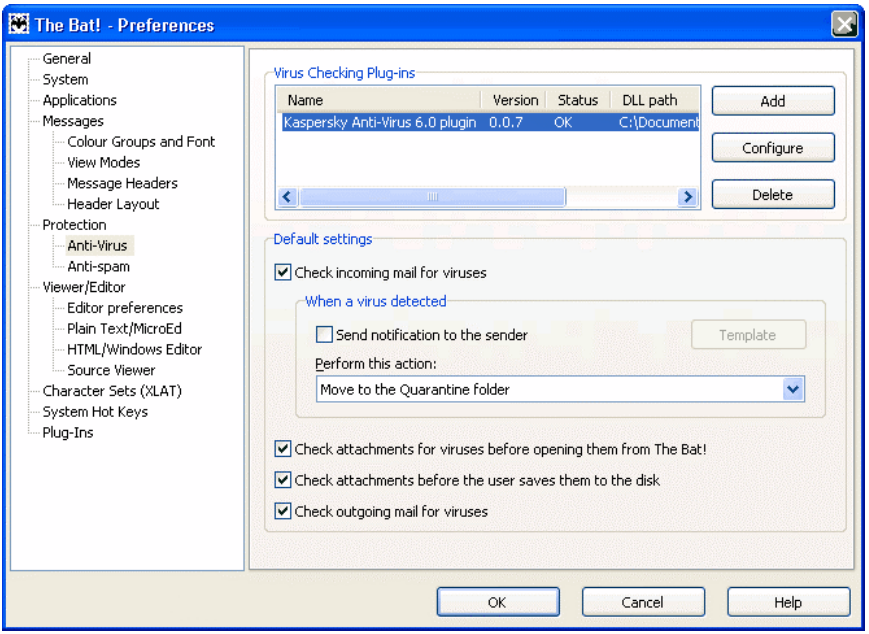


Illustration 25. Configuration du courrier dans The Bat!

Vous devez définir :

- Le flux de messagerie qui sera soumis à l'analyse antivirus (courrier entrant, sortant);
- Le moment auquel aura lieu l'analyse antivirus des objets du message (à l'ouverture du message, avant l'enregistrement sur le disque);
- Les actions exécutées par le client de messagerie en cas de découverte d'objets dangereux dans les messages électroniques. Vous pouvez par exemple choisir :

  Tenter de réparer les parties infectées : tente de réparer l'objet infecté du message; si la réparation est impossible, l'objet reste dans le message. Kaspersky Internet Security vous avertira obligatoirement si l'objet du message électronique est infecté. Même si vous choisissez **Supprimer** dans la fenêtre de notification de l'antivirus de messagerie électronique, l'objet restera dans le message car l'action à réaliser sur le message, sélectionnée dans The Bat! prévaut sur l'action de l'antivirus de messagerie électronique.

Supprimer les parties infectées : supprime l'objet dangereux du message, qu'il soit infecté ou soupçonné d'être infecté.

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

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

8.2.4. Restauration des paramètres de protection du courrier par défaut

Lorsque vous configurez Antivirus Courrier, vous avez toujours la possibilité de revenir aux paramètres recommandés par les experts de Kaspersky Lab et regroupés sous le niveau **Recommandé**.

Pour restaurer les paramètres de protection du courrier par défaut :

1. Sélectionnez **Antivirus Courrier** dans la fenêtre principale et cliquez sur le lien Configuration pour passer à la fenêtre de configuration du composant.
2. Cliquez sur **Par défaut** dans la section **Niveau de protection**

8.2.5. Sélection des actions à réaliser sur les objets dangereux des messages

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

A la fin de l'analyse, chaque objet peut se voir attribuer l'un des statuts suivants :

- Etat de l'un des programmes malveillants (exemple, *virus, cheval de Troie*), pour de plus amples renseignements, consultez le point 1.2 à la page 11);
- *Potentiellement infecté* lorsqu'il n'est pas possible d'affirmer avec certitude si l'objet est infecté ou non. Cela signifie que le code du message contient une séquence semblable à celle d'un virus connu mais modifié ou qui évoque la séquence d'un virus.

Par défaut, l'antivirus de messagerie affiche un message par défaut en cas de découverte d'un objet dangereux et potentiellement infecté et propose un choix d'actions.

Pour modifier l'action à exécuter sur l'objet :

Ouvrez la fenêtre de configuration de Kaspersky Internet Security et sélectionnez **Antivirus Courrier**. Toutes les actions envisageables sont reprises dans le bloc **Action** (cf. ill. 26).

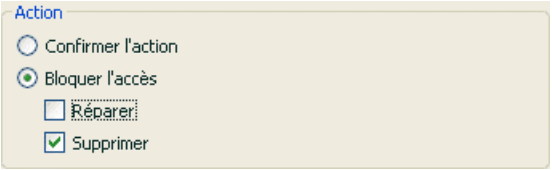


Illustration 26. Sélection de l'action à réaliser sur l'objet dangereux du message

Examinons en détails les différentes options en matière de traitement des objets dangereux des messages électroniques.

Action choisie	Résultat de l'action
Confirmer l'action	L'antivirus Courrier affiche un message d'avertissement (cf. point 5.9, p. 66) qui reprend les informations relatives à l'objet malveillant source de l'infection (potentielle) et propose l'une des actions suivantes.
Ne pas confirmer l'action	L'antivirus Courrier ne traitera pas l'objet. Les informations relatives sont consignées dans le rapport (cf. point 16.3, p. 237). Vous pouvez plus tard tenter de réparer cet objet.
Ne pas confirmer l'action **Réparer**	L'antivirus Courrier exécute l'une des actions suivantes : Tentative de réparation de l'objet infecté. Si la réparation a réussi, vous pourrez à nouveau travailler avec cet objet. Si la réparation échoue, l'accès à l'objet sera bloqué. Les informations relatives à cette situation sont consignées dans le rapport. Il est possible de tenter de réparer cet objet ultérieurement.

Action choisie	Résultat de l'action
	Placement de l'objet potentiellement infecté en quarantaine. Plus tard, il sera possible de tenter de récupérer l'objet ou de le rétablir dans son emplacement d'origine.
Ne pas confirmer l'action **Réparer** **Supprimer si la réparation n'est pas possible**[2]	L'antivirus Courrier exécute l'une des actions suivantes : Tentative de réparation de l'objet infecté. Si la réparation a réussi, vous pourrez à nouveau travailler avec cet objet. Si la réparation a échoué. Placement de l'objet potentiellement infecté par le virus en quarantaine (cf. point 16.1, p. 231).
Ne pas confirmer l'action **Réparer** **Supprimer**	En cas de découverte d'un objet infecté ou potentiellement infecté, l'antivirus Courrier le supprime sans prévenir l'utilisateur.

Quel que soit le statut de l'objet (infecté ou potentiellement infecté), Kaspersky Internet Security crée une copie de sauvegarde avant de tenter de le réparer ou de le supprimer. Cette copie est placée dans le dossier de sauvegarde (cf. point 16.2, p. 235) au cas où il faudrait restaurer l'objet ou si la réparation devenait possible.

[2] Si vous utilisez The Bat! en tant que client de messagerie, les objets dangereux des messages seront soit réparés, soit supprimé avec cette action de l'antivirus de messagerie électronique (en fonction de l'action sélectionnée dans The Bat!).

CHAPITRE 9. PROTECTION INTERNET

Chaque fois que vous utilisez Internet, vous exposez votre ordinateur à un risque d'infection par des programmes dangereux. Ceux-ci peuvent se charger sur votre ordinateur pendant que vous ouvrez le site ou que vous lisez certains articles en ligne.

Pour garantir la sécurité de vos données lorsque vous utilisez Internet, Kaspersky Internet Security propose un composant spécial : l'antivirus Internet. Il protège les informations reçues via le protocole HTTP et empêche l'exécution des scripts dangereux.

Attention !

La protection Internet prévoit le contrôle du trafic http qui transite uniquement via les ports indiqués dans la liste des ports contrôlés (cf. point 16.7, p. 259). La liste des ports le plus souvent utilisés pour le transfert du courrier et du trafic HTTP est livrée avec le logiciel. Si vous utilisez des ports absents de cette liste, vous devrez les ajouter afin de protéger le trafic qui transite via ces derniers.

Si vous travaillez dans un domaine non protégé (connexion à Internet via un modem), il est conseillé d'utiliser l'antivirus Internet en guise de protection. Si votre ordinateur fonctionne dans un réseau protégé par un pare-feu ou un filtre de trafic HTTP, l'antivirus Internet vous offrira une protection supplémentaire.

L'icône de Kaspersky Internet Security dans la barre des tâches indique le fonctionnement du composant. Cette icône prend cette apparence  chaque fois qu'un script est analysé.

Examinons les détails du fonctionnement de ce composant.

l'antivirus Internet est composé de deux modules qui garantissent :

- La *protection du trafic HTTP* : analyse de tous les objets qui arrivent sur l'ordinateur via le protocole HTTP.
- *Analyse des scripts* : analyse de tous les scripts Java et Visual Basic lancés sur l'ordinateur pendant le travail de l'utilisateur, y compris sur Internet.

  S'agissant de Microsoft Internet Explorer, il existe un plug-in spécial qui s'intègre au programme lors de l'installation de Kaspersky Internet Security. L'icône  qui apparaît dans la barre d'outils du navigateur confirme l'installation du plug-in. En cliquant sur cette icône, vous ouvrez

un panneau qui reprend les statistiques d'Anti-Virus sur le nombre de scripts bloqués et analysés.

La protection du trafic HTTP s'opère selon l'algorithme suivant :

1. Chaque page ou fichier qui reçoit une requête de l'utilisateur ou d'un programme quelconque via le protocole HTTP est intercepté et analysé par l'antivirus Internet pour découvrir la présence de code malveillant. L'identification des objets malveillants est réalisée à l'aide des *signatures de menaces* utilisées par Kaspersky Internet Security et d'un algorithme heuristique. Les signatures contiennent la définition de tous les programmes malveillants connus à ce jour et de leur mode d'infection. L'algorithme heuristique permet d'identifier les nouveaux virus dont les définitions ne sont pas encore reprises dans les signatures de menaces.
2. Les comportements suivants sont possibles en fonction des résultats de l'analyse :
    a. Si la page Web ou l'objet que souhaite ouvrir l'utilisateur contient un code malveillant, l'accès est bloqué. Dans ce cas, un message apparaît à l'écran pour avertir l'utilisateur que l'objet ou la page demandée est infecté.
    b. Si aucun code malveillant n'a été découvert dans le fichier ou la page Web, l'utilisateur pourra y accéder immédiatement.

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

1. Chaque script lancé sur une page Web est intercepté par l'antivirus Internet et soumis à une analyse antivirus.
2. Si le script contient un code malveillant, l'antivirus Internet le bloc et avertit l'utilisateur à l'aide d'une infobulle.
3. Si le script ne contient aucun code malicieux, il est exécuté.

9.1. Sélection du niveau de sécurité Internet

Kaspersky Internet Security assure la protection de votre utilisation d'Internet selon un des 3 niveaux suivants (cf. ill. 27):

Elevé : le contrôle des scripts et des objets reçus via le protocole HTTP est total. Le logiciel analyse en détail tous les objets à l'aide des signatures complètes. Ce niveau de protection est recommandé dans les environnements agressifs lorsque aucun autre moyen de protection du trafic HTTP n'est utilisé.

Recommandé : les paramètres de ce niveau correspondent aux paramètres recommandés par les experts de Kaspersky Lab. L'analyse porte sur les mêmes objets que ceux du niveau **Elevé**, si ce n'est que la durée de mise en cache des fragments de fichier est restreinte, ce qui permet d'accélérer l'analyse et le transfert des objets à l'utilisateur.

Faible : la configuration de ce niveau de protection vous permet de travailler sans problèmes avec les applications gourmandes en mémoire vive car le volume d'objets analysés est réduit vu l'utilisation d'un ensemble restreint de signatures de menaces. L'utilisation de ce niveau est recommandée uniquement si d'autres moyens de protection du trafic Internet sont installés sur votre ordinateur.

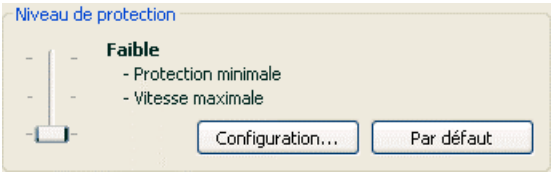


Illustration 27. Sélection du niveau de protection d'Internet

Par défaut, la protection des fichiers s'opère selon les paramètres du niveau **Recommandé**.

Vous pouvez augmenter ou réduire le niveau de protection du courrier en sélectionnant un autre niveau ou en modifiant les paramètres du niveau actuel.

Pour modifier le niveau de protection :

Déplacez simplement le curseur. Ce faisant, vous modifiez le rapport entre la vitesse de l'analyse et la quantité d'objets analysés : plus le nombre d'objets soumis à la recherche de code malveillant sera réduit, plus la vitesse de l'analyse sera élevée

Si un des niveaux ne correspond pas à vos besoins, vous pouvez créer le niveau **Utilisateur.** Voici des exemples de situations où cela pourrait s'imposer :

Exemple:

Votre ordinateur se connecte à Internet via modem. Il ne fait pas partie du réseau local et la protection antivirus du trafic HTTP entrant est absente.

Dans le cadre de vos activités professionnelles, vous téléchargez souvent de gros fichiers. L'analyse de tels fichiers prend en général un certain temps.

Comment protéger au maximum votre ordinateur contre une infection via le trafic HTP ou les scripts ?

Conseil pour la sélection du niveau :

l'analyse de la situation permet de conclure que votre ordinateur fonctionne dans un niveau agressif et que le risque d'infection via le trafic HTTP est très élevé (absence de protection centralisée du trafic Internet et des moyens d'accès à Internet).

Dans ce cas, il est conseillé d'utiliser le niveau **Elevé** qui sera modifié de la manière suivante : il est conseillé de limiter dans le temps la mise en cache des fragments de fichiers lors de l'analyse.

Pour modifier les paramètres du niveau de protection proposé par défaut :

cliquez sur **Configuration** dans la fenêtre des paramètres de l'antivirus Internet, modifiez les paramètres de la protection Internet (cf. point 9.2, p. 116) selon vos besoins et cliquez sur **OK**.

9.2. Configuration de la protection Internet

La protection Internet analyse tous les objets téléchargés sur votre ordinateur via le protocole HTTP et assure le contrôle de tous les scripts Java et Visual Basic lancés.

Vous pouvez configurer différents paramètres de l'antivirus Internet afin d'accélérer la vitesse de fonctionnement du composant, notamment :

- Définir l'algorithme d'analyse, en choisissant la sélection complète ou partielle des signatures des menaces.
- indiquer les objets du trafic HTTP qu'il ne faudra pas soumettre à la recherche d'objets dangereux;
- composer la liste des adresses dont le contenu est fiable.

Vous pouvez également sélectionner les actions que l'antivirus Internet exécutera sur les objets du trafic HTTP.

Tous ces types de paramètres sont abordés en détails ci-après.

9.2.1. Définition de l'algorithme d'analyse

L'analyse des données reçues via Internet peut s'opérer selon l'un des deux algorithmes suivants :

- *Analyse continue* : technologie d'identification du code malveillant dans le trafic du réseau qui procède à l'analyse "en vol" des données. Supposons

que vous téléchargiez un fichier depuis un site Web. L'antivirus Internet analyse le fichier au fur et à mesure du téléchargement. Cette technologie accélère la livraison de l'objet analysé à l'utilisateur. L'analyse continue recours à un nombre restreint de signatures des menaces (uniquement les plus actives), ce qui réduit considérablement la sécurité de l'utilisation d'Internet.

- *Analyse avec mise en tampon* : technologie d'identification du code malveillant dans le trafic du réseau qui procède à l'analyse de l'objet une fois qu'il a été entièrement copié dans la mémoire tampon. Après cela, l'objet est soumis à l'analyse antivirus et, en fonction des résultats, est transmis à l'utilisateur ou est bloqué. Ce type d'analyse exploite toutes les signatures des menaces, ce qui augmente considérablement la probabilité d'identifier tout code malveillant. Toutefois, cette technologie s'accompagne d'une augmentation du temps de traitement de l'objet et de son transfert à l'utilisateur. Il peut également y avoir des problèmes en cas de copie et de traitement d'objets volumineux suite à l'expiration du délai de connexion au client http. Afin d'éviter de tels inconvénients, nous vous conseillons de limiter la mise en cache des fragments de l'objet reçu via Internet. Une fois ce délai écoulé, chaque partie du fichier reçue sera transmise directement à l'utilisateur. L'objet aura été analysé entièrement à la fin de la mise en cache. Cela permet d'accélérer la vitesse de transfert de l'objet, d'éviter les problèmes liés aux déconnexions, le tout, sans réduire le niveau de protection de l'ordinateur.

Afin de sélectionner l'algorithme d'analyse qui sera suivi par l'antivirus Internet :

1. Cliquez sur **Configuration** dans la fenêtre de configuration de l'antivirus Internet.
2. Sélectionnez la valeur adéquate dans le bloc **Algorithme d'analyse** de la fenêtre qui s'affiche (cf. ill. 28).

Par défaut, l'antivirus Internet analyse les données avec mise en tampon et en utilisant les signatures des menaces complètes. La durée de mise en cache des fragments du fichier est également limitée à 1 seconde.

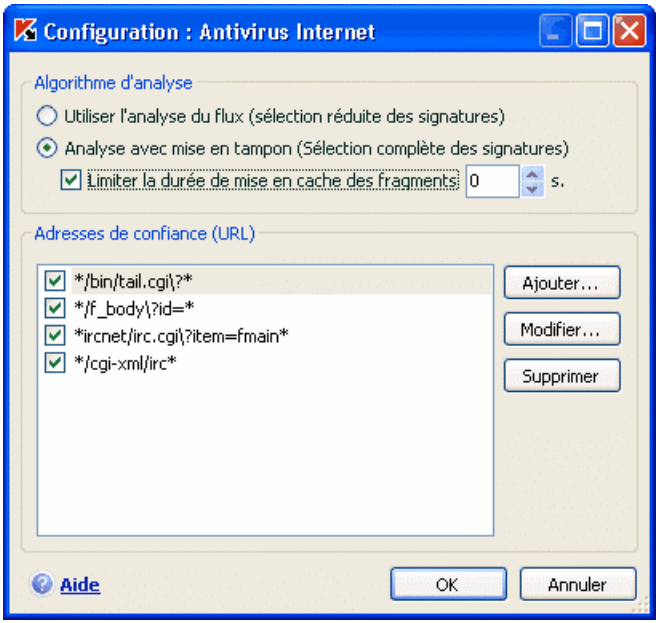


Illustration 28. Configuration du niveau de protection Internet

Attention !

Si vous écoutez la radio ou regardez la télévision via Internet ou si vous participez à des téléconférences en ligne et que vous êtes souvent confronté à des problèmes relatifs à la validité de l'objet requis, utilisez l'algorithme d'analyse des flux.

9.2.2. Constitution de la liste des adresses de confiance

Vous pouvez créer une liste d'adresses de confiance pour lesquelles vous n'avez absolument aucun doute au niveau du contenu. Les informations issues de ces adresses ne seront pas soumises à la recherche d'objets dangereux. Cela peut être utile lorsque l'antivirus Internet gêne l'utilisation normale d'Internet, par exemple le téléchargement d'un certain fichier qui est à chaque fois bloqué par l'antivirus Internet.

Pour constituer la liste des adresses de confiance :

1. Cliquez sur **Configuration** dans la fenêtre de configuration de l'antivirus Internet.
2. Composez, dans la fenêtre qui s'ouvre (cf. ill. 28), la liste des serveurs de confiance dans la zone **Adresses de confiance (URL)**. Utilisez pour ce faire les boutons situés à droite.

Lors de la saisie d'une adresse de confiance, vous pouvez choisir un masque à l'aide des caractères spéciaux suivants :

***** : n'importe quelle séquence de caractères.
Exemple : le masque ***abc*** signifie que toute adresse contenant la séquence **abc** ne sera pas analysée, par exemple www.virus.com/download_virus/page_0-9abcdef.html.

? : n'importe quel caractère.
Exemple : le masque **Patch_123?.com** signifie que l'adresse contenant cette séquence de caractères suivie de n'importe quel caractère après le "3" ne sera pas analysée, par exemple **Patch_1234.com**. Toutefois, l'adresse **patch_12345.com** sera quant à elle analysée.

Au cas où les caractères ***** et **?** feraient partie d'une URL authentique ajoutée à la liste, il est indispensable d'ajouter également le caractère **** qui annule le caractère *****, **?**ou **** qui le suit

Exemple : il faut absolument ajouter à la liste des adresses de confiance l'URL suivante : www.virus.com/download_virus/virus.dll?virus_name=

Afin que Kaspersky Internet Security n'interprète pas **?** comme un symbole d'exclusion, il faut le faire précéder du caractère \. Ainsi, notre URL ajoutée à la liste des adresses de confiance deviendra : www.virus.com/download_virus/virus.dll\?virus_name=

9.2.3. Restauration des paramètres de protection Internet par défaut

Lorsque vous configurez Antivirus Internet, vous avez toujours la possibilité de revenir aux paramètres recommandés par les experts de Kaspersky Lab et regroupés sous le niveau **Recommandé**.

Pour restaurer les paramètres de protection Internet par défaut :

1. Sélectionnez **Antivirus Internet** dans la fenêtre principale et cliquez sur le lien Configuration pour passer à la fenêtre de configuration du composant.
2. Cliquez sur **Par défaut** dans la section **Niveau de** protection

9.2.4. Sélection des actions à réaliser sur les objets dangereux

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

Pour configurer la réaction de l'antivirus Internet suite à la découvert d'un objet dangereux :

Ouvrez la fenêtre de configuration de Kaspersky Internet Security et sélectionnez **Antivirus Internet**. Toutes les actions envisageables sont reprises dans le bloc **Action** (cf. ill. 29).

Par défaut, l'antivirus Internet affiche un message par défaut en cas de découverte d'un objet dangereux et suspect et propose un choix d'actions.

Illustration 29. Sélection de l'action à réaliser sur le script dangereux

Examinons en détails les différentes options en matière de traitement des objets dangereux présents dans le trafic HTTP.

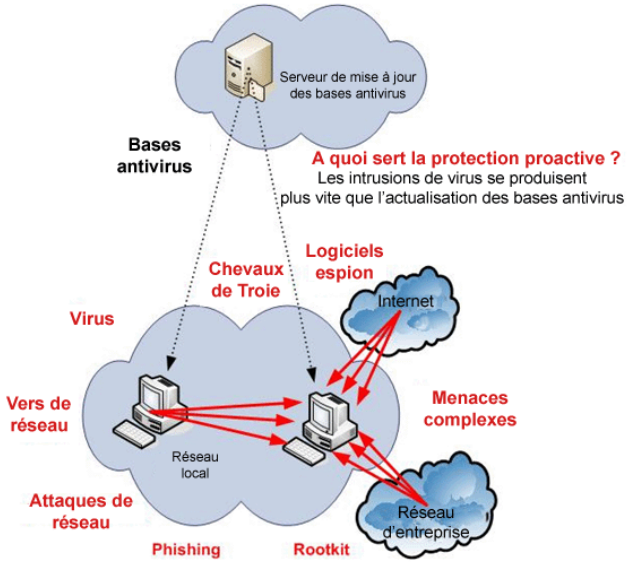
Action choisie	Résultat en cas de découverte d'un objet dangereux dans le trafic http.
Confirmer l'action	L'antivirus Internet affiche un message d'avertissement qui reprend les informations relatives au code malveillant source de l'infection et propose l'une des actions suivantes.
Bloquer	L'antivirus Internet bloque l'accès à l'objet et affiche un message signalant le blocage. Ces informations sont également reprises dans le rapport (cf. point 16.3, p. 237).
Autoriser	L'antivirus Internet autorise l'accès à l'objet dangereux. Les informations sont consignées dans le rapport.

S'agissant des actions sur les scripts dangereux, l'antivirus Internet bloque toujours leur exécution et affiche à l'écran une infobulle qui informe l'utilisateur sur l'action exécutée. Vous ne pouvez pas modifier l'action exécutée sur un script suspect ou dangereux, si ce n'est désactiver le fonctionnement du module d'analyse des scripts.

CHAPITRE 10. DEFENSE PROACTIVE DE L'ORDINATEUR

Kaspersky Internet Security offre non seulement une protection contre les menaces connues, mais également contre les menaces récentes qui ne sont pas encore reprises dans les bases des signatures des menaces. Cet aspect de la protection est pris en charge par un composant particulier : la *défense proactive*.

La nécessité d'une défense proactive a vu le jour dès le moment où la vitesse de propagation des programmes malveillants a dépassé la vitesse de mise à jour des protections antivirus capables de neutraliser ces menaces. Les technologies réactives de protection contre les virus requièrent au minimum une infection par la nouvelle menace, le temps nécessaire à l'analyse du code malveillant, à son ajout dans les bases des signatures des menaces et à la mise à jour de celles-ci sur l'ordinateur de l'utilisateur. Tout cela laisse suffisamment de temps à la nouvelle menace pour causer des dégâts irréparables.



Les technologies préventives sur lesquelles reposent la défense proactive de Kaspersky Internet Security évitent ces pertes de temps et permettent de

neutraliser la nouvelle menace avant qu'elle n'ait pu nuire à votre ordinateur. Comment est-ce possible ? A la différence des technologies réactives qui réalisent l'analyse selon le code, les technologies préventives identifient les nouvelles menaces sur votre ordinateur en suivant les séquences d'actions exécutées par certaines applications (processus). Le logiciel est livré avec un ensemble de critères qui permettent de définir la dangerosité d'une activité. Si l'activité d'une application quelconque évoque les actions d'une activité dangereuse, l'application est immédiatement considérée comme dangereuse et elle est soumise à l'action prévue dans les règles pour une telle activité. Voici quelques exemples d'activités dangereuses :

- Modifications du système de fichiers ;
- Intégration de modules dans d'autres processus ;
- Processus cachés ;
- Modification des clés de la base de registres système de Microsoft Windows.

Toutes les opérations dangereuses sont surveillées et bloquées par la défense proactive.

La défense proactive surveille également toutes les macros VBA exécutées dans les applications Microsoft Office. Les signatures des menaces sont utilisées pour définir le caractères malveillant d'une macro.

La défense proactive fonctionne selon une série de règles reprises dans le programme et d'exclusions définies. Une *règle* est en ensemble de critères qui définit le niveau de danger d'une activité quelconque et la réaction du logiciel face à une telle activité.

Des règles distinctes sont prévues pour l'activité de l'application et contrôlent les modifications de la base de registres système, les macros et les processus lancés sur l'ordinateur. Vous pouvez modifier la liste des règles et en ajouter de nouvelles voire supprimer ou modifier certaines. Les règles peuvent interdire ou autoriser.

Voici l'algorithme de fonctionnement de la défense proactive :

1. Directement après le démarrage de l'ordinateur, la défense proactive analyse les aspects suivants :
    - *Actions de chaque application exécutée sur l'ordinateur*. L'historique des actions exécutées et leur séquences sont enregistrées et comparées aux séquences caractéristiques des activités dangereuses (la base des types d'activités dangereuses est intégrée au logiciel et elle est actualisée en même temps que les signatures des menaces).

- *Actions de chaque macro VBA lancée*. Le composant vérifie si elles sont reprises dans la liste des actions dangereuses livrée avec le logiciel.
- *Intégrité des modules logiciels* des applications installées sur l'ordinateur, ce qui permet d'éviter la substitution de modules, l'insertion de code malveillant ou le lancement de ces applications par des codes malveillants.
- *Chaque tentative de modification de la base de registres système* (suppression ou ajout de clé à la base de registres système, saisie de valeurs étranges pour les clés, etc.),

2. L'analyse s'opère selon les règles de la défense proactive et des exclusions définies.
3. Les comportements suivants sont possibles en fonction des résultats de l'analyse :
   - Si l'activité répond aux conditions prévues par la règle d'autorisation de la défense proactive, elle ne sera pas bloquée.
   - Si l'activité est décrite dans une règle d'interdiction, la suite de l'action du composant est régie par les instructions reprises dans la règle. En règle générale, une telle action est bloquée. Il est possible qu'une notification apparaisse à l'écran. Celle-ci reprend l'application, le type d'activité et l'historique des actions exécutées. Vous devrez décider vous-même d'autoriser ou non une telle action. Vous pouvez créer une règle pour une telle activité et annuler les actions exécutées dans le système.
   - Si la séquence d'activités exécutées sur l'ordinateur n'est régie par aucune règle, elle sera autorisée.

10.1. Configuration de la défense proactive

La défense proactive s'exécute dans le respect stricte de paramètres (cf. ill. 30) qui définissent si :

- *L'activité des applications est contrôlée sur votre ordinateur*.

  Ce mode de fonctionnement est réglementé par la case **Activer l'analyse**. Le mode est activé par défaut, ce qui garantit un suivi rigoureux de l'activité de n'importe quel programme lancé sur l'ordinateur. Il existe une sélection d'activités dangereuses. Pour chacune d'entres elles, vous pouvez configurer l'ordre de traitement des applications (cf.

point 10.1.1, p. 126) avec une telle activité. Il est possible également de créer des exclusions, ce qui permet d'annuler le contrôle de l'activité pour certaines applications.

- *Le contrôle de l'intégrité de l'application est activé.*

  Ce service est responsable de l'intégrité des modules des applications installées sur l'ordinateur et est réglementé par la case **Activer le contrôle de l'intégrité**. L'intégrité est surveillée via le contrôle de la composition des modules du processus et de la somme de contrôle du processus en question. Vous pouvez créer des règles pour l'exécution d'actions concrètes par ce processus. Si l'application n'est pas reprise dans la liste des applications contrôlées, son intégrité et sa composition ne seront pas contrôlées.

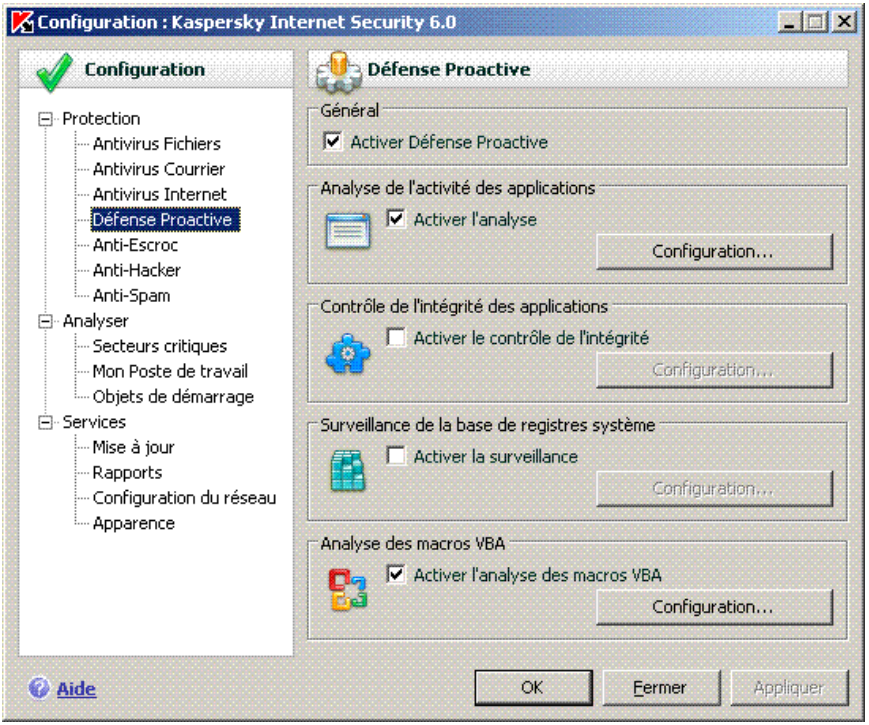


Illustration 30. Paramètres de la défense proactive

- *Le contrôle des modifications de la base de registres système est assuré.*

  La case **Activer la surveillance** est cochée, ce qui signifie que Kaspersky Internet Security analyse soigneusement toutes les tentatives

de modifications des clés contrôlées dans la base de registres système du système d'exploitation.

Vous pouvez créer vos propres règles (cf. point 10.1.4.2, p. 138) de contrôle en fonction de la clé de registre.

- *L'analyse des macros est réalisée*.

  Le contrôle de l'exécution des macros sur l'ordinateur est réglementé par la case **Activer l'analyse des macros VBA**. Cette case est cochée par défaut, et par conséquent, toutes les actions des macros Visual Basics for Applications sont soumises à un contrôle strict de la part de la défense proactive.

  Vous pouvez sélectionner les macros que vous estimez dangereuses et comment les traiter (cf. point 10.1.3, p. 133).

Vous pouvez configurer les exclusions (cf. point 6.3.1, p. 76) pour les modules de la défense proactive et composer des listes d'applications de confiance (cf. point 6.3.2, p. 81).

Tous ces paramètres sont abordés en détails ci-après.

10.1.1. Règles de contrôle de l'activité

Toutes les applications de votre ordinateur sont soumises à la stricte observation de Kaspersky Internet Security. La case **Activer le contrôle** régit le contrôle de l'activité

Le programme contient une sélection d'actions dangereuses opérée sur la base d'études approfondies des spécialistes de Kaspersky Lab. Une règle est créée pour chaque type d'activité dangereuse. Si l'activité d'une application est considérée comme dangereuse, la défense proactive suivra à la lettre les instructions reprises dans la règle prévue pour ce type d'activité.

Voici quelques exemples d'activités dangereuses :

- *Lancement du navigateur avec les paramètres.* Une telle activité est caractéristique pour le lancement de Microsoft Internet Explorer depuis une application quelconque avec les clés de la ligne de commande. Par exemple, ce type d'action est exécuté si vous cliquez sur un lien vers une page Web quelconque dans un message électronique que vous avez reçu. Il s'agit du lancement du navigateur selon quelques paramètres. Une telle activité est répandue parmi les programmes malveillants. Toutefois, une telle activité n'est pas toujours nuisible.

- *Implantation dans un autre processus* : ajout dans le processus d'un programme d'un code quelconque issu d'un autre programme. Cette activité est très répandue parmi les chevaux de Troie mais elle

accompagne également l'installation sur votre ordinateur de programmes tout à fait inoffensif ou de mises à jour.

- *Intrusion d'intercepteurs de fenêtre.* Cette activité se manifeste lors de la tentative de lecture de mots de passe ou d'autres informations confidentielles que vous saisissez à l'aide du clavier. Il existe néanmoins toute une série de logiciels dans lesquels la saisie d'informations depuis le clavier est une fonction tout à fait normale, par exemple les dispositifs automatiques de reconnaissance du clavier.

La liste des activités dangereuses est remplie automatiquement lors de la mise à jour de Kaspersky Internet Security et il est impossible de la modifier. Vous pouvez :

- refuser de contrôler une activité quelconque en désélectionnant la case  qui se trouve en regard de son nom.
- modifier la règle qui définit le fonctionnement de la défense proactive lors de la découverte d'activités dangereuses.
- composer une liste d'exclusions (cf. point 6.3, p. 75)reprenant les applications que vous n'estimez pas dangereuses.

Pour passer à la configuration du contrôle de l'activité :

1. Ouvrez la fenêtre des paramètres de Kaspersky Internet Security en cliquant sur Configuration dans la fenêtre principale.
2. Sélectionnez **Défense proactive** dans l'arborescence des paramètres.
3. Cliquez sur le bouton **Configuration** dans le bloc **Analyse de l'activité des applications**.

Les activités dangereuses contrôlées par la défense proactive sont reprises dans la fenêtre **Configuration: analyse de l'activité** (cf. ill. 31).

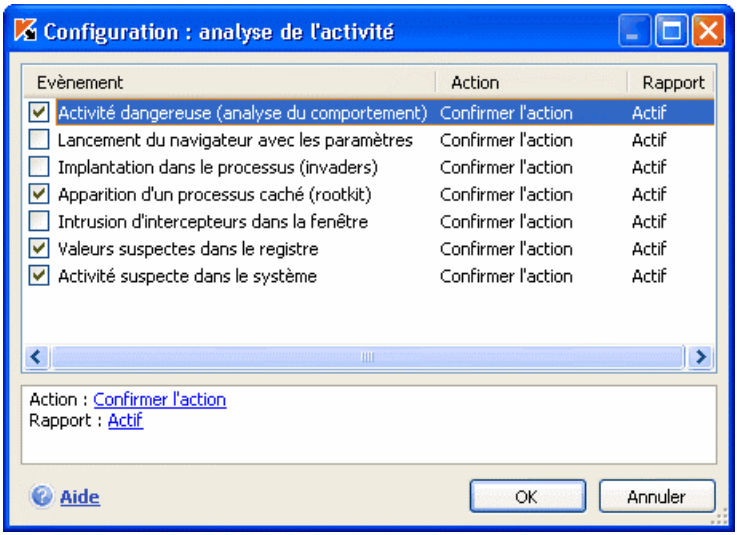


Illustration 31. Configuration du contrôle de l'activité des applications.

Pour modifier une règle de contrôle de l'activité dangereuse, sélectionnez-la dans la liste de l'onglet **Evénements** et définissez dans la partie inférieure de la fenêtre les paramètres de la règle :

- Définissez la réaction de la défense proactive suite à la découverte d'une activité dangereuse.
- Vous pouvez sélectionner une des actions suivantes en guise de réaction : autoriser, confirmer l'action et terminer le processus. Cliquez avec le bouton gauche de la souris sur le lien de l'action jusqu'à ce qu'il prenne la valeur souhaitée. De plus, à la fin de l'exécution du processus, vous pouvez le placer en quarantaine. Pour ce faire, cliquez sur On / Off en regard du paramètre correspondant.
- Indiquez la nécessité de créer un rapport sur l'opération exécutée. Pour ce faire, cliquez sur On / Off.

Afin de ne pas contrôler une activité dangereuse quelconque, désélectionnez la case ☑ qui se trouve en regard de son nom dans la liste des applications dangereuses. Les activités de ce type ne seront plus soumises à l'analyse de la défense proactive.

10.1.2. Contrôle de l'intégrité de l'application

Il existe de nombreux logiciels qui peuvent entraîner des conséquences sérieuses lorsque du code malveillant s'y intègre, par exemple une violation de l'intégrité du système, etc. En règle générale, il s'agit d'application système, de processus utilisés pour se connecter à Internet ou lors de l'utilisation du courrier ou d'autres documents. C'est pour cette raison que ces applications sont considérées comme *critiques* d'un point de vue du contrôle de leur activité.

La défense proactive assure un contrôle rigoureux de tels applications. Elle analyse leur activité, le lancement d'autres processus par des applications critiques. Kaspersky Internet Security est livré avec une liste d'applications critiques et chacune d'entre elles possède sa propre règle de contrôle. Vous pouvez ajouter à cette liste d'autres applications que vous jugez critiques de même que modifier les règles pour les applications reprises dans la liste.

Il existe également un ensemble de modules de confiance. Il s'agit par exemple des modules qui possèdent la signature de Microsoft Corporation. Il est fort probable que les applications qui contiennent de tels modules ne soient pas malveillantes. Pour cette raison, il n'est pas nécessaire de soumettre leurs actions à un contrôle strict. Les experts de Kaspersky Lab ont composé une liste de ces modules afin de réduire la charge de votre ordinateur lors du fonctionnement de la défense proactive.

Les composants qui possèdent la signature Microsoft Corporation sont repris par défaut automatiquement dans la liste des applications de confiance. Le cas échéant, vous pouvez ajouter ou supprimer des éléments à cette liste.

Le contrôle des processus dans le système est activé en cochant la case ☑ **Activer le contrôle de l'intégrité**. La case est n'est pas sélectionnée par défaut. En cas de contrôle de l'intégrité chaque application ou module lancé est analysé afin de voir s'il se trouve dans la liste des applications critiques ou des applications de confiance. Si l'application appartient à la liste des applications critiques, son activité sera soumise à un contrôle strict de la part de la défense proactive conformément à la règle définie.

Pour passer à la configuration du monitorage des processus :

1. Ouvrez la fenêtre des paramètres de Kaspersky Internet Security en cliquant sur Configuration dans la fenêtre principale.
2. Sélectionnez **Défense proactive** dans l'arborescence des paramètres.
3. Cliquez sur le bouton **Configuration** dans le bloc **Contrôle de l'intégrité des applications**.

Examinons plus en détail le fonctionnement avec les processus critiques et les processus de confiance.

10.1.2.1. Configuration des règles de contrôle des applications critiques

Les *applications critiques* sont les fichiers exécutables des programmes dont il est primordial de contrôler l'activité dans la mesure où l'insertion de code malveillant au sein de tels programmes peut avoir des conséquences sérieuses.

Une liste d'applications critiques, composée par les experts de Kaspersky Lab et livrée avec le logiciel, est reprise sur l'onglet **Applications contrôlées** (cf. ill. 32). Une règle de contrôle est créée pour chacune de ces applications. Vous pouvez créer vos propres règles ou modifier les règles existantes.

La défense proactive analyse les opérations suivantes dans les applications critiques : lancement, modification de la composition des modules de l'application et lancement de l'application en tant que processus fils. Pour chacune des opérations citées, vous pouvez sélectionner la réaction de la défense proactive (autoriser ou non l'opération) et préciser s'il est nécessaire de consigner l'activité dans le rapport de fonctionnement du composant. Par défaut, le lancement, la modification et le lancement de processus fils pour pratiquement toutes les applications critiques sont autorisés.

Afin d'ajouter une application critique à la liste et de créer une règle de contrôle :

1. Cliquez sur le bouton **Ajouter** dans l'onglet **Applications contrôlées**. Cette action entraîne l'ouverture d'un menu contextuel. Le point **Parcourir** ouvre la boîte de dialogue traditionnelle pour la sélection des fichiers. Vous pouvez également cliquer sur le point **Applications** afin d'afficher la liste des applications ouvertes à ce moment et de sélectionner celle que vous voulez. L'application prendra la première place dans la liste. Une règle d'autorisation sera créée par défaut. Lors du premier lancement de l'application, une liste des modules utilisés au lancement est créée. Ce sont ces modules qui seront autorisés.

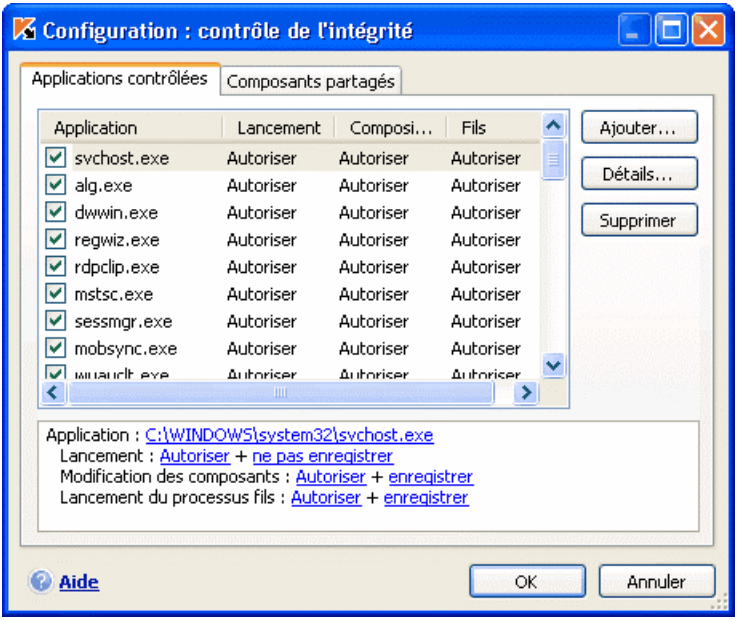


Illustration 32. Configuration du contrôle de l'intégrité de l'application

2. Sélectionnez la règle dans la liste et définissez-en les paramètres dans la partie inférieure de l'onglet :

   - Définissez la réaction de la défense proactive en cas de tentative de lancement, de modification de la composition ou de lancement d'une application critique en tant que processus fils.

     Vous pouvez sélectionner une des actions suivantes en guise de réaction : autoriser, confirmer l'action et interdire. Cliquez avec le bouton gauche de la souris sur le lien de l'action jusqu'à ce qu'il prenne la valeur souhaitée.

   - Indiquez la nécessité de créer un rapport sur l'opération exécutée. Pour ce faire, utilisez le lien enregistrer / ne pas enregistrer.

Pour désactiver le contrôle de l'activité d'une application critique quelconque, il suffit de désélectionner la case ☑ qui se trouve en regard de son nom.

10.1.2.2. Création de la liste des composants partagés

Kaspersky Internet Security prévoit une liste de composants partagés qui peuvent être chargés dans toutes les applications contrôlées. Cette liste est reprise sur l'onglet **Composants partagés** (cf. ill. 33). La liste contient les modules utilisés par Kaspersky Internet Security, les composants qui possèdent la signature de Microsoft Corporation et les composants ajoutés par l'utilisateur.

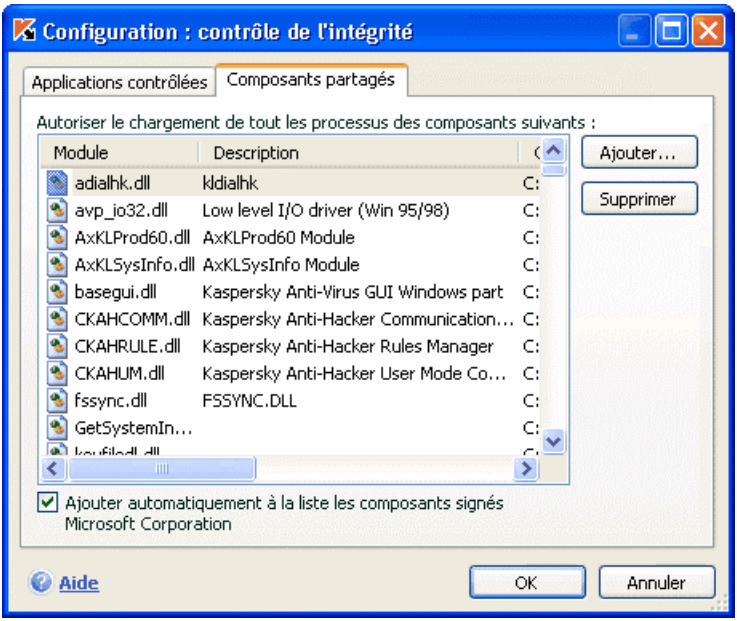


Illustration 33. Configuration de la liste des modules de confiance

Vous pouvez installer différents programmes sur votre ordinateur et si vous souhaitez que les modules accompagnés de la signature de Microsoft Corporation soient ajoutés automatiquement à la liste des modules de confiance, cochez la case **Ajouter automatiquement à la liste des composants signés Microsoft Corporation**. Dans ce cas, si l'application contrôlée souhaite charger un module possédant la signature de Microsoft Corporation, le chargement de ce module sera accepté automatiquement et le module sera placé dans la liste des composants partagés.

Pour ajouter des modules de confiance, cliquez sur **Ajouter** et sélectionnez les modules souhaités dans la boîte de dialogue traditionnelle de sélection des fichiers.

10.1.3. Contrôle de l'exécution des macros VBA

L'analyse et le traitement des macros dangereuses lancées sur votre ordinateur est garanti lorsque la case ☑ **Activer l'analyse des macros VBA** est cochée. La case est cochée par défaut, ce qui signifie que toute macro lancée est analysée et si celle-ci appartient à la liste des macros dangereuses, elle est traitée de la manière adéquate.

Exemple:

> La barre Adobe Acrobat, intégrée à Microsoft Office Word, permet de créer des fichiers PDF au départ de n'importe quel document grâce à la macro *PDFMaker*. La défense proactive considère les actions telles que l'intégration d'éléments dans un programme comme dangereuses. Si le contrôle des macros est activé, Kaspersky Internet Security affichera un message d'avertissement à l'écran en cas d'exécution de la macro pour vous signaler qu'une macro dangereuse a été découverte. Vous pourrez alors décider soit d'arrêter l'exécution de la macro, soit l'autoriser.

Vous pouvez configurer les actions à suivre lorsque la macro exécute certaines actions et créer une liste des exclusions qui reprendra les macros qui, pour vous, ne présentent aucun danger. Ces macros ne seront pas analysées par la défense proactive.

Pour passer à la configuration de l'analyse des macros :

1. Ouvrez la fenêtre des paramètres de Kaspersky Internet Security en cliquant sur Configuration dans la fenêtre principale.
2. Sélectionnez **Défense proactive** dans l'arborescence des paramètres.
3. Cliquez sur le bouton **Configuration** dans le bloc **Analyse des macros VBA**.

La configuration des règles de traitement des macros dangereuses s'opère sur l'onglet **Configuration de l'analyse des macros VBA** (cf. ill. 34). Par défaut, il contient les règles applicables aux macros dont les actions sont considérées comme dangereuses par les experts de Kaspersky Lab. Il s'agit par exemple de l'insertion de modules dans un programme, de la suppression de fichiers, etc.

Chaque macro est associée à une action qui sera exécutée par Kaspersky Internet Security suite à la découverte de la macro.

Si vous estimez que l'action d'une macro quelconque ne représente aucun danger, désélectionnez la case en regard de son nom. Par exemple, vous travaillez en permanence avec un logiciel qui exécute une macro pour l'ouverture

de plusieurs fichiers en écriture et vous êtes absolument certain que cette opération n'est pas dangereuse.

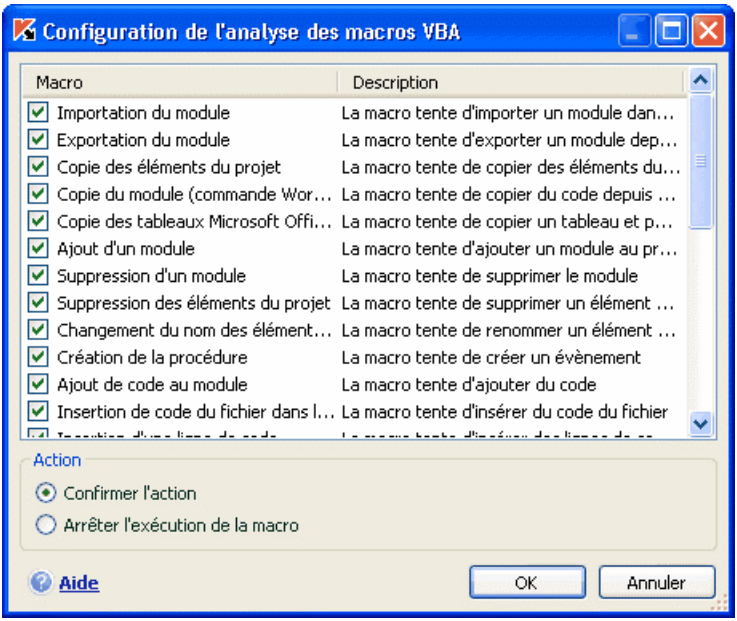


Illustration 34. Configuration des paramètres d'analyse des macros VBA

Afin que Kaspersky Internet Security ne bloque pas l'exécution de la macro :

désélectionnez la case en regard de l'action correspondante. Cette macro ne sera plus considérée comme dangereuse et sera exécutée sans hésitation.

Par défaut, chaque fois que le programme découvre une macro dangereuse sur l'ordinateur, il affiche un message à l'écran pour confirmer l'autorisation ou non de l'exécution de la macro.

Afin que le programme bloque automatiquement l'exécution de toutes les macros sans demander l'avis préalable de l'utilisateur :

sélectionnez le traitement **Arrêter l'exécution de la macro** dans la fenêtre reprenant la liste des macros.

10.1.4. Contrôle des modifications de la base de registres système

La modification de la base de registres système du système d'exploitation de votre ordinateur est le but poursuivi par de nombreux programmes malveillants. Il peut s'agir de jokewares inoffensifs ou d'autres programmes malveillants qui représentent une véritable menace pour votre ordinateur.

Ainsi, un jokeware pourrait s'inscrire dans la clé de registre responsable du lancement automatique des applications. Directement après le démarrage du système d'opération de l'ordinateur, vous pouvez voir sur l'écran un message qui vous prévient que votre ordinateur est infecté alors que ce n'est pas le cas.

S'agissant des chevaux de Troie, ils peuvent, après avoir modifié la base de registres système, non seulement accéder aux ressources mais également nuire à l'intégrité du système de l'ordinateur.

La défense proactive, et tout particulièrement le module spécial activé en cochant la case ☑ **Activer la surveillance**, vous permet de découvrir des menaces encore inconnues qui tenteraient de modifier les clés.

Pour passer à la configuration du contrôle de la base de registres système :

1. Ouvrez la fenêtre des paramètres de Kaspersky Internet Security en cliquant sur Configuration dans la fenêtre principale.
2. Sélectionnez **Défense proactive** dans l'arborescence des paramètres.
3. Cliquez sur le bouton **Configuration** dans le bloc **Surveillance de la base de registres système**.

La liste des règles qui régissent la manipulation des clés du registre a déjà été dressée par les experts de Kaspersky Lab et elle est reprise dans le fichier d'installation. Les opérations sur les clés de registres sont réparties en groupes logiques tels que *System security*, *Internet Security*, etc. Chacun de ces groupes contient les clés de la base de registres système et les règles de manipulation de celles-ci. Cette liste est augmentée de nouveaux groupes de règles pour les clés lors de la mise à jour du logiciel.

La liste complète des règles est prise sur l'onglet **Groupes de clés de registres** (cf. ill. 35).

Chaque groupe possède une priorité d'exécution que vous pouvez augmenter ou diminuer à l'aide des boutons **Monter** et **Descendre**. Si une même clé est reprise dans plusieurs groupes, la première règle qui sera appliquée à la clé sera la règle du groupe dont la priorité est la plus élevée.

Utilisez l'une des méthodes suivantes pour annuler l'utiliser d'un groupe de règles quelconque :

- Désélectionnez la case ☑ en regard du nom du groupe. Dans ce cas, le groupe de règles demeure dans la liste, mais il n'est plus utilisé par la défense proactive.
- Supprimez le groupe de règles de la liste. Il n'est pas conseiller de supprimer les groupes de règles créés par les experts de Kaspersky Lab car ils contiennent les sélections optimales de règles.

Illustration 35. Groupe de clés de la base de registres système contrôlées

Si le groupe de règles pour les clés ne correspond pas parfaitement à vos critères de contrôle de la base de registres système, vous pouvez créer vos propres règles. Pour ce faire, cliquez sur **Ajouter** dans la fenêtre du groupe de clés.

Exécutez les actions suivantes dans la fenêtre ouverte :

1. Saisissez le nom du nouveau groupe de règles de contrôle des clés de la base de registres système dans le champ **Nom**.
2. Constituez la liste des clés (cf. point 10.1.4.1, p. 137) de la base de registres système pour lesquelles vous souhaitez créer des règles dans l'onglet **Règles**. Il peut s'agir d'une seule clé ou de plusieurs.
3. Sur l'onglet **Règles**, créez une règle (cf. point 10.1.4.2, p. 138) pour les clés du registre. Vous pouvez créer plusieurs règles de traitement et définir leur priorité.

10.1.4.1. Sélection des clés de registre pour la création de règles

Lors de l'ajout de clé de la base de registres système au groupe, vous pouvez indiquer une clé ou un groupe de clés. La règle peut être créée pour la clé ou pour sa valeur particulière.

La liste des clés pour la règle est rédigée sur l'onglet **Clés**.

Afin d'ajouter une clé de la base de registres système :

1. Cliquez sur **Ajouter** dans la boîte de dialogue **Modification du groupe** (cf. ill. 36).
2. Dans la boîte de dialogue qui s'ouvre, sélectionnez la clé ou le groupe de clés de la base de registres système pour laquelle vous voulez créer une règle de contrôle.
3. Indiquez dans le champ **Valeur** la valeur de la clé ou le masque du groupe de clés auquel vous souhaitez appliquer la règle.
4. Cochez la case **Clés intégrées comprises** afin que la règle s'applique à toutes les clés intégrées de la clé de la base de registres système sélectionnée pour la règle.

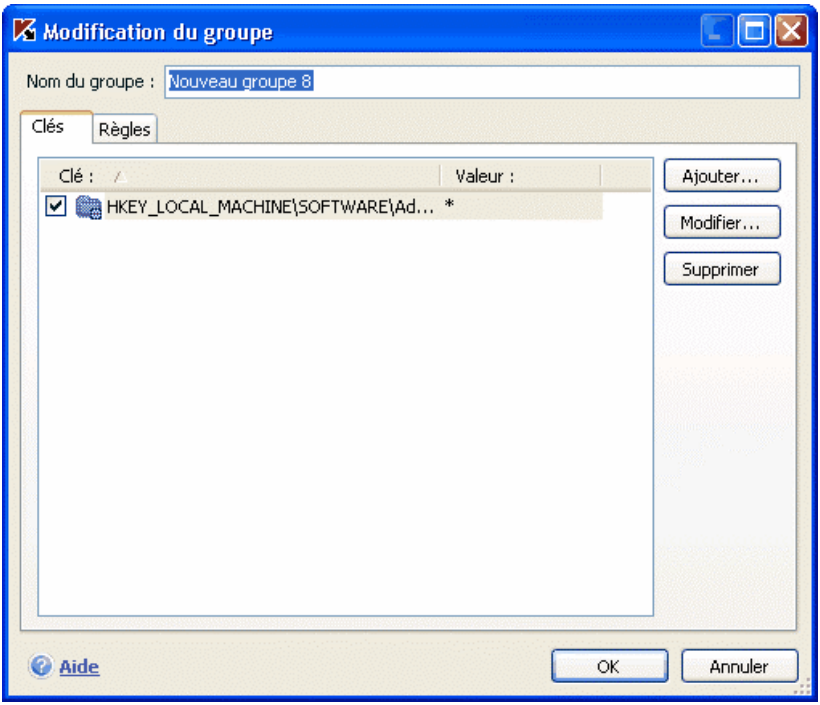


Illustration 36. Ajout d'une clé à contrôler

L'utilisation simultanée d'un masque avec les caractères * ou ? et de l'option **Clés intégrées comprises** s'impose uniquement si ces caractères figurent dans le nom de la clé.

Si un groupe de clé dans le registre a été sélectionné à l'aide d'un masque et qu'une règle concrète a été définie, celle-ci sera appliquée à la valeur indiquée pour n'importe quelle clé du groupe sélectionné.

10.1.4.2. Création d'une règle de contrôle des clés du registre

La règle de contrôle des clés de la base de registres système est basée sur la définition de :

- l'application à laquelle la règle sera appliquée si elle adresse une requête à la clé de la base de registres système;

- des réactions du programme en cas de tentative de la part de l'application d'exécuter une opération quelconque avec la clé de la base de registres système.

Ainsi, afin de créer une règle pour les clés de la base de registres système sélectionnées :

1. Cliquez sur **Créer** dans l'onglet **Règles**. La règle générale sera ajoutée en tête de liste (cf. ill. 37).

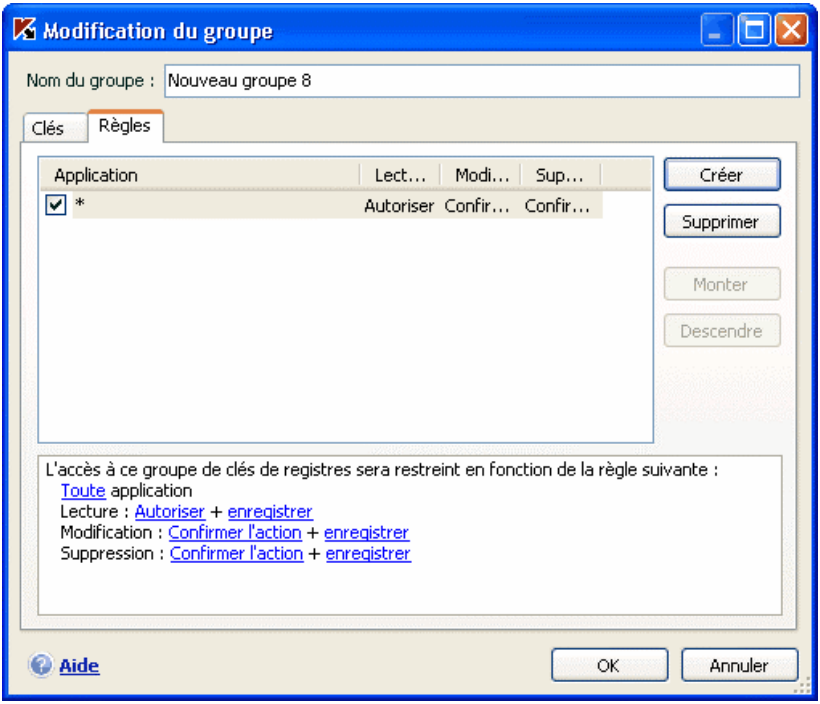


Illustration 37. Création d'une règle de contrôle des clés de la base de registre système

2. Sélectionnez la règle dans la liste et définissez-en les paramètres dans la partie inférieure de l'onglet :

   - Précisez l'application.

     Par défaut, une règle est créée pour chaque application. Afin que la règle soit appliquée à un programme concret, cliquez avec le bouton gauche de la souris sur le lien quelconque. Il devient sélectionné. Cliquez ensuite sur le lien indiquez l'application. Cette action entraîne l'ouverture d'un menu

contextuel. Le point **Parcourir** ouvre la boîte de dialogue traditionnelle pour la sélection des fichiers. Vous pouvez également cliquez sur le point **Applications** afin d'afficher la liste des applications ouvertes à ce moment et de sélectionner celle que vous voulez.

- Définissez la réaction de la défense proactive lorsque l'application sélectionnée tente de lire, de modifier ou de supprimer les clés de la base de registres système.

  Vous pouvez sélectionner une des actions suivantes en guise de réaction : autoriser, confirmer l'action et interdire. Cliquez avec le bouton gauche de la souris sur le lien de l'action jusqu'à ce qu'il prenne la valeur souhaitée.

- Indiquez la nécessité de créer un rapport sur l'opération exécutée. Pour ce faire, utilisez le lien enregistrer / ne pas enregistrer.

Vous pouvez créer quelques règles et définir la priorité de leur application à l'aide des boutons **Monter** et **Descendre**.

Il est possible également de créer une règle d'autorisation pour la clé de la base de registres système au départ de la notification sur la tentative d'exécution d'une opération sur la clé. Pour ce faire, cliquez sur Créer une règle d'autorisation et dans la boîte de dialogue qui s'ouvre, précisez le champ d'application de la règle.

CHAPITRE 11. PROTECTION CONTRE LES PUBLICITES ET LES ESCROQUERIES EN LIGNE

Parmi les applications dangereuses qui se répandent de plus en plus ces derniers temps, il faut citer les programmes dont les objectifs sont les suivants :

- Vol de vos données confidentielles (mots de passe, numéro de carte de crédit, documents importants, etc.);
- Suivi des actions réalisées sur l'ordinateur, analyse des programmes installés;
- Publicité envahissante dans les fenêtres du navigateur, les fenêtres pop up et les bannières de différents programmes;
- Accès non-autorisé à Internet depuis votre ordinateur pour consulter des sites au contenu divers.

Les attaques de phishing et l'interception des frappes de clavier visent à voler des informations tandis que les dialers vers des sites Internet payant, les jokewares et les adwares entraînent des pertes de temps et d'argent. C'est précisément de ces logiciels que l'Anti-Escroc vous protège.

Anti-Escroc contient les modules suivants :

- *Anti-phishing* vous protège contre les attaques de phishing.

  En règle générale, les attaques de phishing sont des messages électroniques prétendument envoyés par une institution financière et qui contiennent des liens vers le site de ces institutions. Le texte du message invite le destinataire à cliquer sur le lien et à saisir des données confidentielles (numéro de carte de crédit, code d'accès aux services de banque en ligne) sur la page qui s'affiche.

  L'exemple type est le message envoyé par la banque dont vous êtes client et qui contient un lien vers un site officiel. En cliquant sur le lien, vous ouvrez en réalité une copie conforme du site Internet de la banque et il arrive même que l'adresse authentique du site s'affiche; dans la majorité des cas, il s'agit d'un site fictif. Toutes vos actions sur ce site sont suivies et pourraient servir au vol de votre argent.

Le lien vers un site de phishing peut être envoyé non seulement par courrier électronique, mais également par d'autres moyens tels que les messages ICQ. Anti-phishing est à l'affût des tentatives d'ouvertures de ces sites fictifs et les bloque.

Les signatures des menaces de Kaspersky Internet Security contiennent les sites connus à l'heure actuelle qui sont utilisés lors des attaques de phishing. Les experts de Kaspersky Lab y ajoutent les adresses fournies par l'organisation internationale de lutte contre le phishing (The Anti-Phishing Working Group). Cette liste est enrichie lors de la mise à jour des signatures des menaces.

- *Anti-publicité* bloque les fenêtres pop up avec des messages publicitaires qui s'ouvrent lors de la visite de divers sites Internet.

  En règle générale, les informations contenues dans ces fenêtres pop up sont inutiles. Ces fenêtres s'ouvrent automatiquement lorsque vous accédez à un site Internet quelconque ou lorsque vous ouvrez une autre fenêtre après avoir cliqué sur un lien. Elles contiennent des publicités et d'autres renseignements que vous n'aviez jamais pensé lire. Anti-popup bloque l'ouverture de telles fenêtres, comme en témoigne le message spécial qui apparaît au-dessus de l'icône du logiciel dans la barre des tâches. Vous pouvez directement au départ de ce message décider si vous souhaitez bloquer ou non la fenêtre.

  > Anti-popup fonctionne correctement avec le module chargé de bloquer les fenêtres pop up dans Microsoft Internet Explorer, livré avec le Service Pack 2 pour Microsoft Windows XP. Un plug-in est intégré pendant l'installation et permet d'autoriser l'ouverture des fenêtres pop-up pendant l'utilisation d'Internet.

  Certains sites ont recours aux fenêtres pop-up afin de fournir un accès plus rapide et plus pratique aux informations. Si vous visitez souvent de tels sites et que l'information contenue dans les fenêtres pop up est importante pour vous, nous vous conseillons de les ajouter à la liste des sites de confiance (cf. point 11.1.1, p. 144). Ainsi, les fenêtres pop up ne seront pas bloquées.

  En cas d'utilisation de Microsoft Internet Explorer, le blocage des fenêtres pop-up s'accompagne de l'icône  dans la barre d'état du navigateur. En cliquant sur cette icône, vous pouvez lever le blocage ou ajouter la l'adresse à la liste des adresses de confiance.

- *Anti-bannière* bloque les informations publicitaires reprises dans les bandeaux publicitaires ou intégrées à l'interface de divers programmes installés sur votre ordinateur.

Non seulement ces bannières ne présentent aucune information utile, mais de plus, elles vous distraient et augmentent le volume de données téléchargées. Antibannière bloque les bannières les plus répandues à l'heure actuelle grâce aux masques livré avec Kaspersky Internet Security. Vous pouvez désactiver le blocage des bannières ou créer vos propres listes de bannières autorisées ou interdites.

Pour intégré Anti-bannière au navigateur **Opera**, ajoutez la ligne suivante au fichier *standard_menu.ini*, dans la section **[Image Link Popup Menu]**:

```
Item, "New banner" = Copy image address & Execute program, "…\Program Files\Kaspersky Lab\Kaspersky Internet Security 6.0\opera_banner_deny.vbs", "//nologo %C"
```

- *Anti-numéroteur automatique* vous protège contre l'utilisation non autorisée des ressources payantes d'Internet.

L'anti-numéroteur automatique fonctionne uniquement sous Microsoft Windows XP et Microsoft Windows 2000.

En règle générale, ces ressources sont des sites Internet à contenu pornographique. Des programmes malveillants spéciaux (les dialers ou numéroteurs automatiques) établissent la connexion via le modem avec de tels sites. En fin de compte, vous devez payer les données que vous n'avez pas demander. Afin de vous protéger contre de telles menaces, l'anti-numéroteur automatique utilise une liste de numéros téléphoniques utilisés pour ce genre de connexion. Il est repris dans les signatures de menaces. N'importe quelle tentative d'utiliser un numéro de cette liste pour accéder à Internet est bloquée. Si vous souhaitez exclure un numéro quelconque de la liste, vous devrez l'inclure dans la liste des numéros de confiance (cf. point 11.1.3, p. 149).

11.1. Configuration d'Anti-Escroc

La protection contre les escroqueries en ligne et les publicités envahissantes couvre tous les programmes qui permettent le vol d'informations confidentielles et d'argent connus à ce jour des experts de Kaspersky Lab. Vous pouvez toutefois procéder à une configuration plus minutieuse du composant, à savoir :

- Créer une liste d'adresses de sites de confiance (cf. point 11.1.1, p. 144) dont les fenêtres pop up ne seront pas bloquées.

- Composer les listes blanche et noire des bannières (cf. point 11.1.2, p. 146).
- Composer une liste des numéros de téléphone de confiance (cf. point 11.1.3, p. 149) qui peuvent être utilisés pour les connexions de type dial-up.

11.1.1. Constitution de la liste des adresses de confiance pour Anti-publicité

Par défaut, Anti-Escroc bloque la majorité des fenêtres pop up qui s'ouvrent automatiquement sans demander votre autorisation. Les seules exclusions sont les fenêtres pop up des sites Internet repris dans la liste de sites de confiance de Microsoft Internet Explorer et des sites du réseau interne (intranet) où vous êtes actuellement enregistré.

Si votre ordinateur tourne sous Microsoft Windows XP Service Pack 2, Microsoft Internet Explorer est doté de son propre dispositif de blocage des fenêtres pop-up. Vous pouvez le configurer en sélectionnant les fenêtres que vous souhaitez bloquer. Anti-Escroc est compatible avec ce dispositif et adhère au principe suivant : en cas de tentative d'ouverture d'une fenêtre pop up, c'est la règle d'interdiction qui sera toujours privilégiée. Admettons que l'adresse d'une fenêtre pop up a été ajoutée à la liste des fenêtres autorisées par Internet Explorer mais qu'elle ne figure pas dans la liste des adresses de confiance d'Anti-popup. Dans ce cas, la fenêtre sera bloquée. Si le navigateur prévoit le blocage de toutes les fenêtres pop up, alors toutes les fenêtres seront en effet bloquées même si elles figurent dans la liste des adresses de confiance d'Anti-popup. Pour cette raison, il est conseillé de procéder à une configuration parallèle du navigateur et d'Anti-popup en cas d'utilisation de Microsoft Windows XP Service Pack 2.

Si vous souhaitez consulter une de ces fenêtres pour une raison quelconque, vous devez l'ajouter à la liste des adresses de confiance. Pour ce faire :

1. Ouvrez la boîte de dialogue de configuration de Kaspersky Internet Security et sélectionnez Anti-Escroc dans l'arborescence des paramètres.
2. Cliquez sur **Sites de confiance** dans la section dédiée au blocage des fenêtres pop up.
3. Dans la boîte de dialogue qui s'ouvre (cf. ill. 38), cliquez sur **Ajouter** et indiquez le masque des sites dont les fenêtres pop up seront acceptées.

> Astuce.
> Les caractères * et ? peuvent servir de masque pour les adresses de confiance.
> Par exemple, le masque http://www.test* exclus les fenêtres pop up de n'importe quel site dont l'adresse commence par la séquence indiquée.

4. Indiquez si les adresses reprises dans la zone de confiance de Microsoft Internet Explorer seront exclues de l'analyse ou s'il s'agit d'adresse de votre réseau local. Le programme les considère comme des adresses de confiance par défaut et ne bloque pas les fenêtres pop up de ces adresses.

La nouvelle exclusion sera ajoutée au début de la liste des adresses de confiance. Si vous ne souhaitez pas utiliser l'exclusion que vous venez d'ajouter, il suffit de désélectionner la case ☑ qui se trouve en regard de son nom. Si vous souhaitez vous défaire complètement d'une exclusion quelconque, sélectionnez-la dans la liste et cliquez sur **Supprimer**.

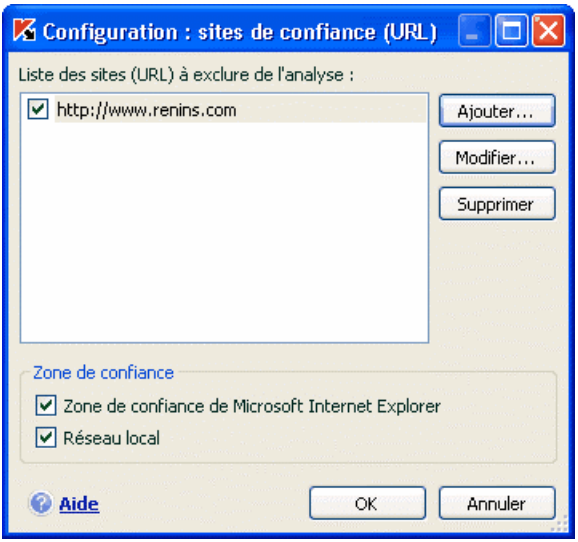


Illustration 38. Constitution de la liste des adresses de confiance

Si vous souhaitez bloquer les fenêtres pop up des sites Web repris dans la liste des sites de confiance pour Microsoft Internet Explorer, désélectionnez les cases adéquates dans la section **Zone de confiance**.

Lors de l'ouverture de fenêtre pop up qui ne figurent pas dans la liste des adresses de confiance, un message apparaît au-dessus de l'icône de l'application et vous informe du blocage. Vous pouvez, à l'aide du lien de ce

message, décider de ne pas bloquer cette adresse et de l'ajouter à la liste des adresses de confiance.

Vous pouvez réaliser une action similaire dans Microsoft Internet Explorer, sous Microsoft Windows XP Service Pack 2. Pour ce faire, utilisez le menu contextuel accessible via l'icône du programme dans la partie supérieure de la fenêtre du navigateur en cas de blocage de fenêtres pop up.

11.1.2. Listes d'adresses de bannières à bloquer

La liste des masques des bannières publicitaires les plus répandues a été constituée par les experts de Kaspersky Lab sur la base d'une étude spéciale et elle est reprise dans l'installation du logiciel. Antibannière vous avertit lorsqu'une bannière publicitaire d'un site ou d'un logiciel a été bloquée. Les bannières qui correspondent à ce masque seront bloquées, pour autant que le blocage n'ait pas été désactivé.

De plus, vous pouvez composer des listes "blanche" ou "noire" de bannières pour décider d'afficher ou non une bannière publicitaire.

L'accès à la racine d'un site n'est pas bloquée si le masque du domaine figure dans la liste "noire" ou dans la liste des bannières interdites.

Admettons que le masque **truehits.net** soit saisi dans la liste des bannières interdites : dans ce cas, il sera toujours possible d'accéder au site **http://truehits.net** mais **http://truehits.net/a.jpg** sera bloqué.

11.1.2.1. Configuration de la liste standard des bannières bloquées

Kaspersky Internet Security contient une liste de masques des bannières les plus répandues que l'on trouve dans les pages Web ou dans les interfaces de divers programmes. Cette liste est constituée par les experts de Kaspersky Lab et elle est actualisée en même temps que les signatures de menaces.

Vous pouvez sélectionner les masques standard de bannières que vous voulez utiliser avec l'antibannière. Pour ce faire :

1. Ouvrez la boîte de dialogue de configuration de Kaspersky Internet Security et sélectionnez Anti-Escroc dans l'arborescence des paramètres.

2. Cliquez sur **Configuration** dans la section chargée du blocage des bannières publicitaires.
3. Ouvrez l'onglet **Général** (cf. ill. 39). Antibannière bloquera les bannières dont le masque est repris sur l'onglet. La séquence de caractères du masque peut être utilisée à n'importe quel endroit de l'adresse de la bannière.

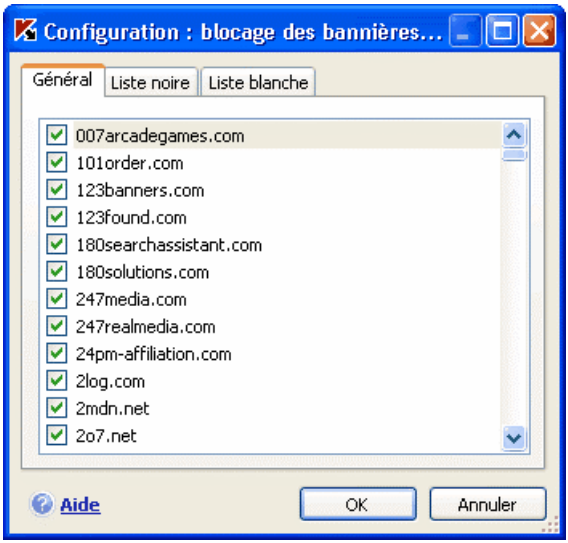


Illustration 39. Liste des bannières bloquées

La liste des masques standard de bannières bloquées ne peut pas être modifiée. Si vous ne souhaitez pas bloquer une bannière qui correspond à un masque standard, vous devrez désélectionner la case ☑ qui se trouve en regard du masque en question.

Vous pouvez également constituer vos propres listes d'adresses autorisées ou interdites. Utilisez pour ce faire les onglets **Liste "blanche"** et **Liste "noire"**.

11.1.2.2. Liste "blanche" de bannières

La liste "blanche" des bannières est composée par l'utilisateur lors de l'utilisation du logiciel afin de ne pas bloquer certaines bannières. Cette liste contient les masques des bannières qui seront affichées.

Pour ajouter un nouveau masque à la liste "blanche" :

1. Ouvrez la boîte de dialogue de configuration de Kaspersky Internet Security et sélectionnez Anti-Escroc dans l'arborescence des paramètres.
2. Cliquez sur le bouton **Configuration** dans la section de blocage des bannières.
3. Ouvrez l'onglet **Liste "blanche"**.

Saisissez, à l'aide du bouton **Ajouter**, le masque de la bannière autorisée dans la liste. Vous pouvez indiquer l'adresse complète de la bannière (URL) ou une suite de caractères. Dans ce cas, cette séquence de caractères sera recherchée en cas de tentative d'affichage d'une bannière.

Pour désactiver un masque saisi sans pour autant le supprimer de la liste, il vous suffira de désélectionner la case ☑ située en regard de ce masque. Les bannières couvertes par ce masque ne seront plus exclues.

Les boutons **Importer** et **Exporter** vous permettent de copier les listes de bannières autorisées d'un ordinateur à un autre.

11.1.2.3. Liste "noire" de bannières

En plus de la liste des masques standard de bannières (cf. point 11.1.2.1, p. 146) bloquées par Antibannière, vous pouvez créer votre propre liste. Pour ce faire :

1. Ouvrez la boîte de dialogue de configuration de Kaspersky Internet Security et sélectionnez Anti-Escroc dans l'arborescence des paramètres.
2. Cliquez sur le bouton **Configuration** dans la section de blocage des bannières.
3. Ouvrez l'onglet **Liste "noire"**.

Saisissez, à l'aide du bouton **Ajouter**, le masque de la bannière que vous souhaitez bloquer. Vous pouvez indiquer l'adresse complète de la bannière (URL) ou une suite de caractères. Dans ce cas, cette séquence de caractères sera recherchée en cas de tentative d'affichage d'une bannière.

Pour désactiver un masque saisi sans pour autant le supprimer de la liste, il vous suffira de désélectionner la case ☑ située en regard de ce masque. Les bannières couvertes par ce masque ne seront plus exclues.

Les boutons **Importer** et **Exporter** vous permettent de copier les listes de bannières bloquées d'un ordinateur à un autre.

11.1.3. Constitution de la liste des numéros de confiance pour Anti-numéroteur automatique

Le module anti-numéroteur automatique contrôle les numéros de téléphone qui servent à l'établissement de connexions Internet cachées. Une connexion cachée est une connexion configurée de telle sorte que l'utilisateur n'en est pas averti ou une connexion que vous n'avez pas ouverte.

Chaque fois qu'une tentative d'ouverture de connexion cachée sera réalisée, un message vous en avertira. Vous serez invité à autoriser ou non cette connexion. Si vous n'avez pas ouvert la connexion, il est fort probable qu'il s'agit d'une action liée à un programme malveillant.

Si vous souhaitez autoriser les connexions via un numéro quelconque sans devoir donner votre confirmation, il faudra ajouter ce numéro à la liste des numéros de confiance. Pour ce faire :

1. Ouvrez la boîte de dialogue de configuration de Kaspersky Internet Security et sélectionnez Anti-Escroc dans l'arborescence des paramètres.
2. Cliquez sur **Numéros de confiance** dans la section dédiée au blocage des numéroteurs automatiques.
3. Dans la boîte de dialogue qui s'ouvre (cf. ill. 40), cliquez sur **Ajouter** et indiquez le numéro ou le masque de numéro pour lequel il ne sera pas nécessaire de bloquer la connexion.

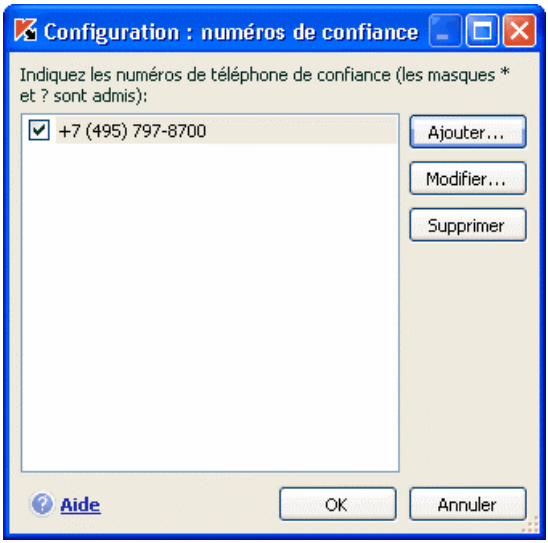


Illustration 40. Constitution de la liste des adresses de confiance

Astuce.

Les caractères * et **?** peuvent servir de masque pour les numéros de confiance.

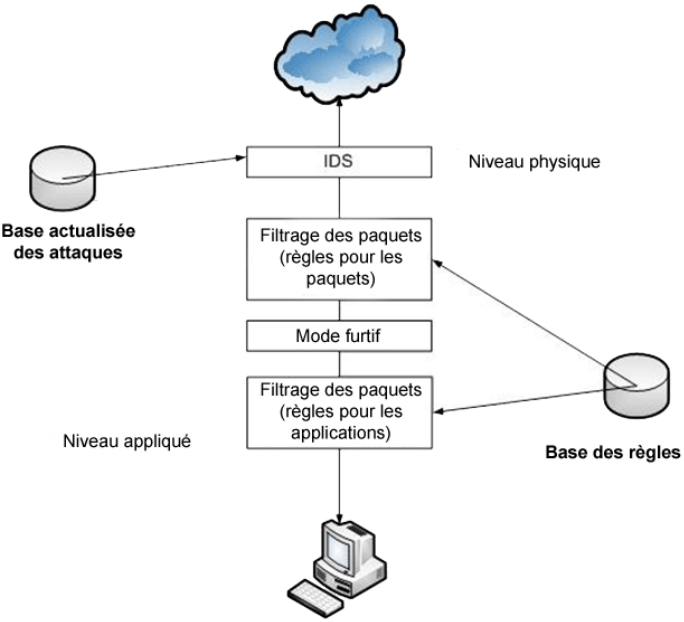
Par exemple, le masque 8????79787* s'appliquera à tous les numéros qui terminent par 79787 et dont le préfixe est composé de trois chiffres quelconque.

La nouvelle exclusion sera ajoutée au début de la liste des numéros de confiance. Si vous ne souhaitez pas utiliser l'exclusion que vous venez d'ajouter, il suffit de désélectionner la case ☑ qui se trouve en regard de son nom. Si vous souhaitez vous défaire complètement d'une exclusion quelconque, sélectionnez-la dans la liste et cliquez sur **Supprimer**.

CHAPITRE 12. PROTECTION CONTRE LES ATTAQUES DE RESEAU

A l'heure actuelle, les ordinateurs sont particulièrement vulnérables lorsqu'ils sont connectés à Internet. Ils sont exposés non seulement aux épidémies de virus, mais également à divers types d'attaques qui exploitent les vulnérabilités des systèmes d'exploitation et des applications.

Afin de protéger votre travail sur les réseaux locaux et sur Internet, Kaspersky Internet Security vous propose un composant spécial : *Anti-Hacker*. Ce composant protège votre ordinateur au niveau du réseau et au niveau des applications et rend votre machine invisible sur le réseau, ce qui permet de déjouer les attaques. Voici une présentation du fonctionnement d'Anti-Hacker.



La protection au niveau du réseau est garantie grâce à l'utilisation de règles globales pour les paquets du réseau qui, suite à l'analyse de paramètres tels que le sens de circulation des paquets, le type de protocole de transfert, le port

d'envoi et de réception du paquet, autorise ou interdit l'activité de réseau. Les règles pour les paquets définissent l'accès au réseau quelles que soient les applications installées sur votre ordinateur qui utilisent le réseau.

En plus des règles pour les paquets, la protection au niveau du réseau est garantie par le *sous-système d'identification des intrusions* (IDS). La tâche de ce sous-système consiste à analyser les connexions entrantes, définir les balayages des ports de l'ordinateur et à filtrer les paquets de réseaux envoyés pour exploiter une vulnérabilité logicielle. Dès que le sous-système d'identification des intrusions s'active, toutes les connexions entrantes émanant de l'ordinateur attaquant seront bloquées pendant une durée déterminée et l'utilisateur sera averti de la tentative d'attaque menée contre son ordinateur.

Le fonctionnement du sous-système de détection des intrusions repose sur l'utilisation pendant l'analyse d'une base spéciale de signatures d'attaques (cf. point 12.9, p. 171) régulièrement enrichie par nos experts et mise à jour en même temps que les signatures des menaces.

La protection au niveau des applications est garantie grâce à l'application de règles d'utilisation des ressources de réseau pour les applications installées sur l'ordinateur. A l'instar de la protection au niveau du réseau, la protection au niveau des applications repose sur l'analyse des paquets de réseau du point de vue du sens de circulation des paquets, du type de protocole de transfert, du port utilisé. Cependant, au niveau de l'application non seulement les caractéristiques du paquet sont prises en compte mais également l'application concrète à laquelle le paquet est destiné ou qui a initialisé l'envoi de ce paquet.

L'utilisation de règles pour les applications permet une configuration plus fine de la protection, par exemple lorsque un type de connexion est interdit pour certaines applications et autorisé pour d'autres.

L'existence de ces deux niveaux de protection fournie par Anti-Hacker entraîne l'existence de deux types de règles :

- *Règles pour les paquets* (cf. point 12.3, p. 160). Ces règles permettent de définir des restrictions générales sur l'activité de réseau quelles que soient les applications installées. Exemple : lors de la création d'une règle pour les paquets qui interdit la connexion sur le port 21, aucune des applications qui utilisent ce port (par exemple, un serveur ftp) ne sera accessible de l'intérieur.

- *Règles pour les applications* (cf. point 12.2, p. 155). Ces règles permettent de définir des restrictions pour l'activité de réseau d'une application particulière. Exemple : si vous avez défini des règles d'interdiction pour le port 80 pour toutes les applications, vous pourrez malgré tout créer une règle qui autorisera une connexion via ce port pour le navigateur FireFox.

Les règles pour les applications et les paquets peuvent être des règles d'*autorisation* ou des règles d'*interdiction*. Le logiciel est livré avec une série de

règles qui régissent l'activité de réseau des applications les plus répandues ainsi que le fonctionnement de l'ordinateur avec les protocoles et les ports les plus utilisés. De plus, cette distribution de Kaspersky Internet Security contient un ensemble de règles d'autorisation pour les applications de confiance dont l'application de réseau ne présente aucun danger.

Afin de faciliter la configuration et l'application des règles dans Kaspersky Internet Security, tout l'espace du réseau a été répartis en deux zones: *Internet* et *zone de sécurité* qui coïncident partiellement avec les sous-réseaux auxquels l'ordinateur est connecté. Vous pouvez attribuer un état à chacune de ces zones (*Internet, Réseau local, Réseau de confiance*) qui définira la politique d'application des règles et de contrôle de l'activité de réseau dans la zone donnée (cf. point 12.5, p. 165).

Le mode *furtif*, qui est un mode de fonctionnement spécial d'Anti-Hacker, complique l'identification de votre ordinateur depuis l'extérieur. Les pirates informatiques sont ainsi privés d'une proie. Ce mode n'a toutefois aucune influence sur votre utilisation d'Internet (pour autant que l'ordinateur ne soit pas utilisé en tant que serveur).

12.1. Sélection du niveau de protection contre les attaques de réseau

Votre utilisation du réseau est protégée selon un des niveaux suivants (cf. ill. 41):

Tout bloquer : niveau de protection qui interdit toute activité de réseau sur votre ordinateur. Lorsque ce niveau est sélectionné, vous ne pouvez utiliser aucune ressource de réseau. Les logiciels qui requièrent une connexion au réseau seront également inutilisables. Il est conseillé de sélectionner ce niveau uniquement en cas d'attaque de réseau ou lorsque l'ordinateur fonctionne dans un milieu dangereux.

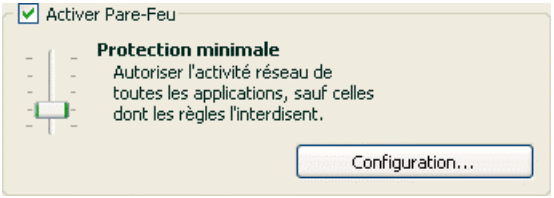


Illustration 41. Sélection du niveau de protection du réseau

Protection maximale : niveau de protection qui accepte les activités de réseau pour lesquelles une règle d'autorisation a été définie. Anti-

Hacker utilise les règles livrées avec le logiciel ou celles que vous avez créées. La sélection de règles livrées avec Kaspersky Internet Security inclut des règles d'autorisation pour les applications dont l'activité de réseau ne suscite aucun doute et pour les paquets de données dont la réception et la transmission ne représente aucun danger. Toutefois, si la liste des règles contient une règle d'interdiction d'une priorité plus élevée que la priorité de la règle d'autorisation, l'activité de réseau de cette application sera interdite.

Attention !

A ce niveau, toute application dont l'activité de réseau n'est pas reprise dans la règle d'autorisation d'Anti-Hacker sera bloquée. Par conséquent, il est conseillé d'utiliser ce niveau uniquement si vous êtes certain que tous les programmes indispensables à votre travail sont autorisés par les règles correspondantes et que vous n'avez pas l'intention d'installer un nouveau logiciel.

Mode d'apprentissage : niveau de protection qui vous permet de définir vous-même les activités de réseau à autoriser ou à interdire. La seule exception se situe au niveau des connexions de réseau pour lesquelles il existent des règles livrées avec le logiciel. Chaque fois qu'un programme quelconque tente d'utiliser une ressource de réseau ou lors du transfert de données, Anti-Hacker vérifie s'il existe une règle pour cette connexion. Si une règle a été définie, Anti-Hacker l'applique strictement. Si aucune règle n'existe, un message d'avertissement apparaît. Ce dernier contient une description de la connexion de réseau (quel programme a été démarré, sur quel port et via quel protocole, etc.). Vous devez décider s'il vaut la peine d'autoriser une telle connexion. A l'aide d'un bouton spécial dans la fenêtre de notification, vous pouvez créer une règle pour cette connexion afin que Anti-Hacker l'applique la prochaine fois qu'une connexion semblable se présentera sans afficher de message.

Protection minimale : niveau de protection qui permet de bloquer l'activité de réseau interdite. Anti-Hacker bloque l'activité en fonction des règles d'interdiction livrées avec le logiciel ou que vous avez créées. La sélection de règles livrées avec Kaspersky Internet Security inclut des règles d'interdiction pour les applications dont l'activité de réseau est dangereuse et pour les paquets de données dont la réception et la transmission représentent un risque. Toutefois, si la liste de règles contient une règle d'autorisation dont la priorité est supérieure à celle de la règle d'interdiction, l'activité de réseau sera autorisée.

Tout autoriser : niveau de protection qui autorise toute activité de réseau sur votre ordinateur. Il est conseillé de sélectionner ce réseau en de très rares occasions uniquement lorsque aucune attaque de réseau n'a

été observée et que vous faites vraiment confiance à n'importe quelle activité de réseau.

Vous pouvez augmenter ou réduire le niveau de protection de l'utilisation du réseau en sélectionnant un autre niveau ou en modifiant les paramètres du niveau actuel.

Pour modifier le niveau de protection du réseau :

1. Sélectionnez **Anti-Hacker** dans la fenêtre de configuration de Kaspersky Internet Security.
2. Dans la partie droite de la fenêtre, déplacez le curseur le long de l'échelle dans la section Pare-feu.

Pour configurer le niveau de protection du réseau :

1. Sélectionnez le niveau de protection qui correspond le plus à vos préférences.
2. Cliquez sur le bouton **Configuration** et modifiez les paramètres de la protection de réseau dans la fenêtre qui s'ouvre.

12.2. Règles pour l'application

Kaspersky Internet Security est livré avec une sélection de règles pour les applications les plus répandues tournant sous le système d'exploitation Microsoft Windows. Plusieurs règles (autorisation ou interdiction) peuvent être rédigées pour une seule et même application. En règle générale, il s'agit de logiciels dont l'activité de réseau a été analysée en détail par les experts de Kaspersky Lab et qui a été clairement jugée comme dangereuse ou non.

En fonction du niveau de protection (cf. point 12.1, p. 153) sélectionné pour le pare-feu et du type de réseau (cf. point 12.5, p. 165) dans lequel l'ordinateur évolue, la liste des règles pour les applications est utilisées différemment. Par exemple, le niveau **Protection maximale** utilise uniquement les règles d'autorisation. Toute l'activité de réseau de l'application qui n'est pas conforme à la règle d'autorisation est bloquée.

Pour manipuler la liste des règles pour l'application

1. Cliquez sur **Configuration** dans la section Pare-feu de la boîte de dialogue de la configuration d'Anti-Hacker.
2. Sélectionnez l'onglet **Règles pour l'application** dans la fenêtre qui s'ouvre (cf. ill. 42).

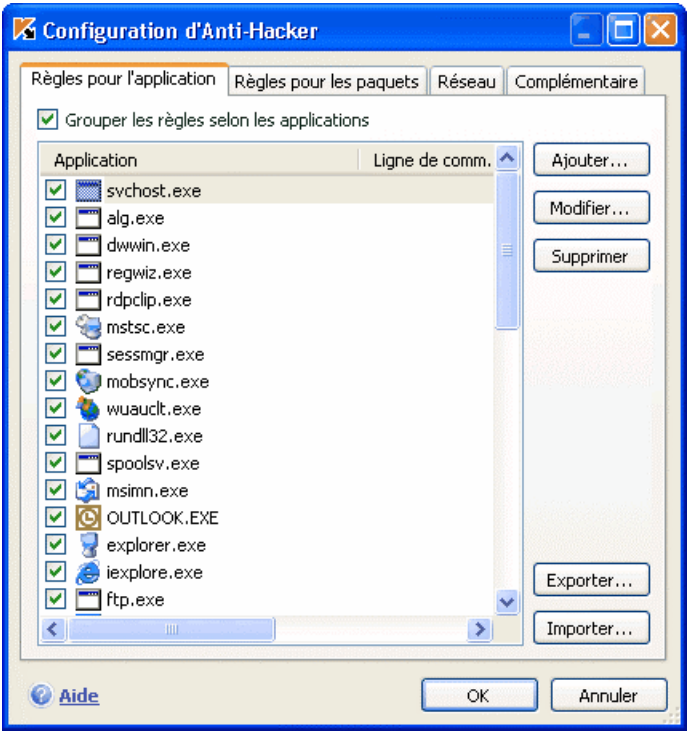


Illustration 42. Liste des règles pour les applications installées.

Toutes les règles reprises sur cet onglet peuvent être regroupées de l'une des manières suivantes :

- *Règles pour l'application*. La case ☑ **Grouper les règles selon les applications** détermine, quand elle est cochée, le regroupement des règles selon ce mode. L'onglet contient la liste des applications pour lesquelles des règles ont été créées. Les informations suivantes accompagnent chaque application : le nom et l'icône de l'application, la ligne de commande, le répertoire racine qui contient le fichier exécutable de l'application et la quantité de règles créées pour elle.

  Le bouton **Modifier** permet de passer à la liste des règles pour l'application sélectionnée et de les modifier : ajouter une nouvelle règle, modifier une règle existante ou la priorité d'exécution.

  Le bouton **Ajouter** permet d'ajouter une nouvelle application à la liste et de créer des règles pour celle-ci.

Les boutons **Exporter** et **Importer** sont prévus pour transférer les règles créées sur un autre ordinateur. Cette option est utile pour procéder à la configuration rapide d'Anti-Hacker.

- *Liste générale des règles* sans regroupement en fonction des applications. Ce mode de présentation de la liste des règles est activé lorsque la case ☑ **Grouper les règles selon les applications** est désélectionnée. La liste générale des règles reprend les informations complètes sur l'application : en plus du nom de l'application et de la ligne de commande nécessaire à son lancement, vous verrez l'action prévue par la règle (autoriser ou non l'activité de réseau), le protocole de transfert des données, le sens du flux de données (entrant ou sortant) et d'autres informations.

  Le bouton **Ajouter** vous permet d'ajouter une nouvelle règle. Le bouton **Modifier** vous permet de passer à la modification de la règle sélectionnée dans la liste. Vous pouvez également modifier les paramètres fondamentaux de la règle dans la partie inférieure de l'onglet.

  Les boutons **Monter** et **Descendre** servent à modifier la priorité d'exécution de la règle.

12.2.1. Création manuelle de règles

Pour créer manuellement une règle pour les applications :

1. Sélectionnez l'application. Pour ce faire, cliquez sur **Ajouter** dans l'onglet **Règles pour l'application**. Sélectionnez dans la fenêtre qui s'ouvre le fichier exécutable de l'application pour laquelle vous souhaitez créer une règle. Cette action entraîne l'ouverture de la liste des règles pour l'application sélectionnée. Si des règles existent déjà, elles seront toutes reprises dans la partie supérieure de la fenêtre. Si aucune règle n'existe, la fenêtre des règles sera vide.

   Il est possible de sélectionner l'application ultérieurement lors de la configuration des conditions de la règle.

2. Cliquez sur **Ajouter** dans la fenêtre des règles pour l'application.

La fenêtre **Nouvelle règle** est un formulaire de création de règles ou vous pouvez configurer des règles (cf. point 12.4, p. 161).

12.2.2. Création d'une règle sur la base d'un modèle

Le logiciel est livré avec des modèles que vous pouvez utiliser pour créer des règles. Ils reprennent les opérations caractéristiques des applications qui ont été minutieusement étudiées par les experts de Kaspersky Lab. Un client de messagerie, par exemple, exécute une série d'opérations standard telles que la réception et l'envoi de courrier. Ces actions sont réalisées grâce à des connexions ouvertes avec le serveur de messagerie via le port et le protocole standard. Au lieu de créer vous-même des règles pour des situations standard comme celles-là, vous pouvez utiliser les modèles.

Afin de rédiger une règle pour une application au départ d'un modèle :

1. Cochez la case **Grouper les règles selon les applications**, si celle-ci avait été désélectionnée, dans l'onglet **Règles pour l'application** et cliquez sur le bouton **Ajouter.**
2. Sélectionnez dans la fenêtre qui s'ouvre le fichier exécutable de l'application pour laquelle vous souhaitez créer une règle. Cette action entraîne l'ouverture de la fenêtre des règles pour l'application sélectionnée. Si des règles existent déjà, elles seront toutes reprises dans la partie supérieure de la fenêtre. Si aucune règle n'existe, la fenêtre des règles sera vide.
3. Dans la fenêtre des règles pour l'application, cliquez sur le bouton **Modèle** et sélectionnez le modèle de règle souhaité dans le menu contextuel (cf. ill. 43).

   Ainsi, **Tout autoriser** est une règle qui autorise n'importe quelle activité de réseau de l'application. Tandis que **Tout interdire** est une règle qui interdit toute activité de réseau de l'application. Toutes les tentatives d'ouverture d'une connexion de réseau par l'application pour laquelle la règle a été créée sera bloquée sans notification préalable de l'utilisateur.

   Les autres modèles repris dans le menu contextuel sont composés de règles caractéristiques pour les programmes correspondant. Le modèle **Client de messagerie**, par exemple, contient une série de règles qui autorisent une activité de réseau standard pour un client de messagerie comme l'envoi de courrier.

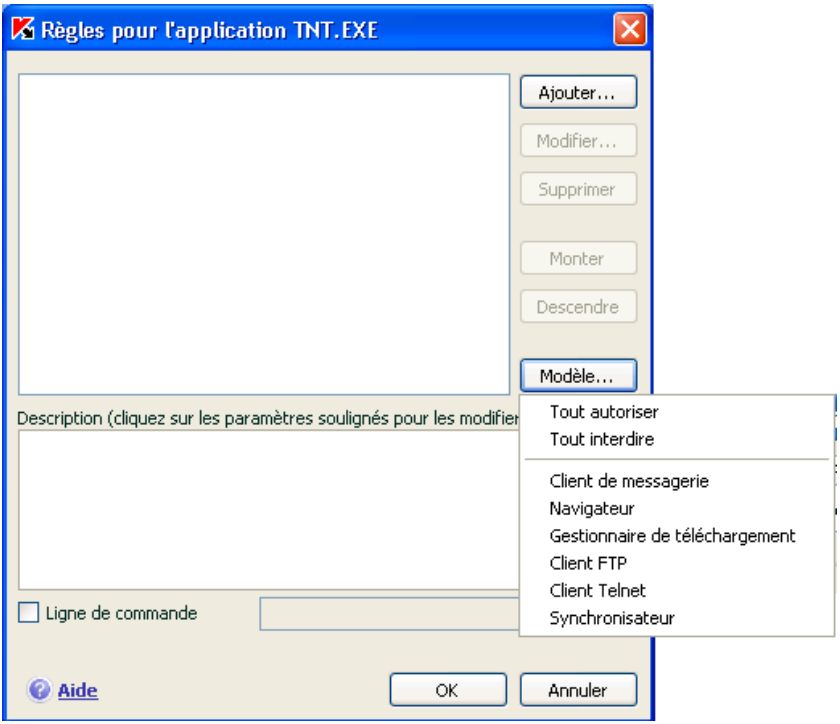


Illustration 43. Sélection du modèle pour la création d'une nouvelle règle

4. Modifiez, le cas échéant, les règles créées pour l'application. Vous pouvez modifier l'action, la direction de la connexion, l'adresse distante, les ports (local et distant) ainsi que l'heure d'activation de la règle.

5. Si vous souhaitez que la règle soit appliquée à l'application lancée avec des paramètres définis dans la ligne de commande, cochez la case ☑ **Ligne de commande** et saisissez la ligne dans le champ à droite.

La règle (ou le groupe de règles) créée sera ajoutée à la fin de liste et possèdera la priorité la plus faible. Vous pouvez augmenter la priorité d'exécution de la règle.(cf. point 12.5, p. 165).

Il est possible également de créer une règle au départ de la boîte de dialogue de notification de la découverte d'une activité de réseau (cf. point 12.10, p. 175).

12.3. Règles pour les paquets

Kaspersky Internet Security propose une sélection de règles prévues pour le filtrage des paquets de données reçus ou transmis par votre ordinateur. Le transfert du paquet peut être réalisé par vous-même ou par une application quelconque installée sur votre ordinateur. Le logiciel est livré avec des règles pour le filtrage des paquets dont le transfert a été analysé en profondeur par les experts de Kaspersky Lab et qui été classé ouvertement comme dangereux ou non.

En fonction du niveau de protection sélectionné pour le pare-feu et du type de réseau dans lequel l'ordinateur évolue, la liste des règles est utilisée différemment. Par exemple, le niveau **Protection maximale** utilise uniquement les règles d'autorisation. Le transfert des paquets qui n'est pas couvert par la règle d'autorisation est bloqué.

Pour manipuler la liste des règles pour les paquets

1. Cliquez sur **Configuration** dans la section Pare-feu de la boîte de dialogue de la configuration d'Anti-Hacker.
2. Sélectionnez l'onglet **Règles pour les paquets** dans la fenêtre qui s'ouvre (cf. ill. 44).

Les informations suivantes accompagnent chaque règle de filtrage : le nom de la règle, l'action (autorisation ou non du transfert du paquet), protocole de transfert des données, direction du paquet et paramètres de la connexion au réseau qui sert pour le transfert du paquet.

Dans cette version, l'utilisation des règles de filtrage est réglementée par la case située en regard du nom.

La manipulation des règles de la liste s'opère à l'aide des boutons situés à droite.

Pour créer une nouvelle règle pour les paquets :

Cliquez sur le bouton **Ajouter** dans l'onglet **Règles pour les paquets**.

La fenêtre **Nouvelle règle** qui s'ouvre est un formulaire de création de règles et elle vous permet de procéder à une configuration affinée de la règle (cf. point 12.4, p. 161).

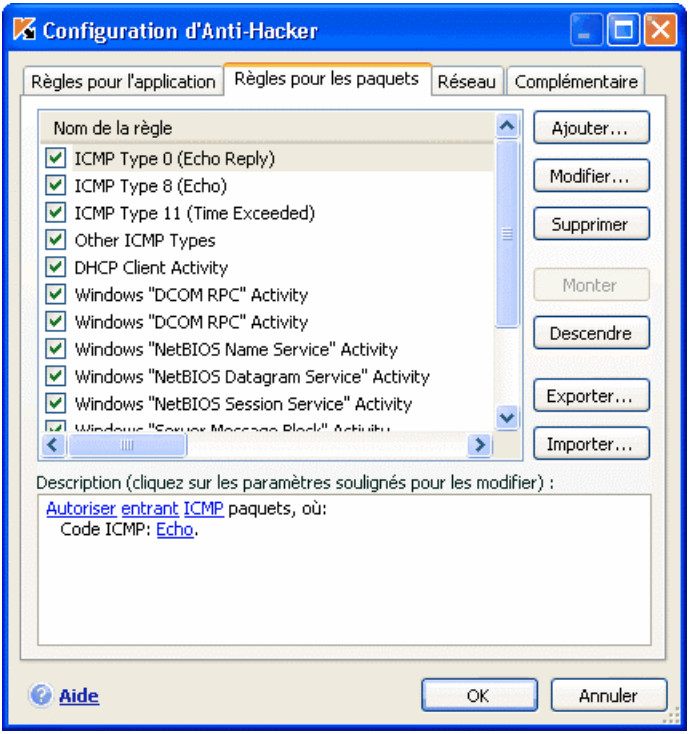


Illustration 44. Liste des règles de filtrage des paquets.

12.4. Configuration affinée des règles pour les applications et les paquets

La fenêtre de configuration affinée des règles **Nouvelle règle** (cf. ill. 45) est pratiquement identique pour les applications et les paquets.

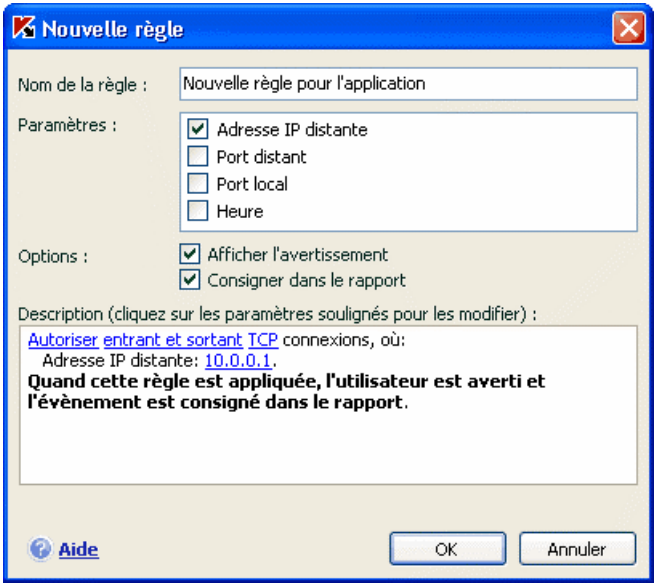


Illustration 45. Création d'une nouvelle règle

La première étape consiste à:

- Définir le nom de la règle. Par défaut, le logiciel utilise un nom standard que vous pouvez modifier.
- Définir les paramètres de la connexion au réseau qui définiront l'application de la règle : adresse distante, port distant, adresse locale, heure. Cochez les cases en regard des éléments que vous voulez exploiter dans la règle.
- Définir les paramètres complémentaires qui alertent l'utilisateur de l'application de la règle. Si vous souhaitez qu'une infobulle apparaisse lors de l'exécution de la règle afin de vous en informer, cochez la case **Afficher l'avertissement**. Afin que les informations relatives à l'exécution de la règle soient consignées dans le rapport d'Anti-Hacker, cochez la case **Consigner dans le rapport**. Par défaut, la case n'est pas cochée lors de la création de la règle. Nous vous conseillons d'utiliser les paramètres complémentaires lors de la création de règles d'interdiction.

La deuxième étape de la création de la règle consiste à définir la valeur de ses paramètres et l'action qui sera exécutée. Tout cela se déroule dans la section **Description**.

a. L'action de chaque règle créée est une action d'*autorisation*. Pour la remplacer par une règle d'interdiction, cliquez avec le bouton gauche de la souris sur Autoriser dans la description de la règle. Le lien devient Interdire.

b. Au cas où vous n'auriez pas choisi une application avant de créer la règle, vous devrez le faire en utilisant le lien précisez l'application. Cliquez avec le bouton gauche de la souris sur le lien et dans la boîte de dialogue standard de sélection des fichiers, choisissez le fichier exécutable de l'application pour laquelle vous créez la règle.

c. Vous devrez ensuite définir la direction de la connexion au réseau pour la règle. Par défaut, la règle est créée aussi bien pour les connexions entrantes que sortantes. Afin de modifier la direction, cliquez avec le bouton gauche de la souris sur entrant et sortant et sélectionnez la direction de la connexion dans la fenêtre qui s'ouvre

   - **Flux entrant.** La règle s'applique uniquement aux connexions de réseau ouvertes par un ordinateur distant et qui visent à transmettre des données quelconque sur votre ordinateur.
   - **Paquet entrant**. La règle s'applique à tous les paquets de données entrants envoyés par un ordinateur distant vers votre ordinateur, à l'exception des paquets TCP.
   - **Flux entrant et sortant**. La règle s'applique aussi bien au flux de données entrant que sortant, quel que soit l'ordinateur (le vôtre ou le poste distant) qui a ouvert la connexion de réseau.
   - **Flux sortant**. La règle s'applique exclusivement aux connexions de réseau ouverte par votre ordinateur et qui transmettent des données quelconque vers l'ordinateur distant.
   - **Paquet sortant**. La règle s'applique à tous les paquets de données transmis par votre ordinateur, à l'exception des paquets TCP.

Si vous devez indiquer dans la règle la direction d'un paquet, précisez s'il s'agit d'un paquet entrant ou sortant. Si vous souhaitez composer une règle pour le flux de données, sélectionnez le type de flux : entrant, sortant ou les deux.

La différence entre *direction du flux* et *direction du paquet* est la suivante : lors de la composition de la règle pour le flux, vous définissez le sens de l'ouverture de la connexion. La direction du paquet lors du transfert de données via cette connexion n'est pas prise en compte.

Admettons que vous ayez configuré une règle pour l'échange de données avec un serveur qui fonctionne en mode FTP passif. Vous devrez autoriser le flux sortant. Pour l'échange de données avec en serveur qui fonctionne selon le mode FTP actif, il est conseillé d'autoriser aussi bien le flux sortant que le flux entrant.

d. Si vous avez sélectionné une adresse distante en guise de paramètre de connexion au réseau, cliquez avec le bouton gauche de la souris sur le lien

précisez l'adresse et dans la fenêtre qui s'ouvre, indiquez l'adresse IP, la plage d'adresses ou l'adresse du sous-réseau. Pour une règle, vous pouvez utiliser un type d'adresse IP ou plusieurs. Il est permis de définir plusieurs adresses de chaque type.

e. Vous devrez ensuite définir le protocole utilisé pour la connexion au réseau. Par défaut, c'est le protocole TCP qui est proposé. Lors de la création de règles pour les applications, vous avez le choix entre deux protocoles : TCP ou UDP. Cliquez avec le bouton gauche de la souris sur le lien représentant le nom du protocole jusqu'à ce qu'il prenne la valeur souhaitée. Si vous créez une règle pour des paquets et que vous souhaitez modifier le type de protocole utilisé par défaut, cliquez sur le lien qui représente son nom et indiquez le protocole requis dans la fenêtre qui s'ouvre. En cas de sélection du protocole ICMP, vous devrez peut-être préciser son type.

   Par exemple, afin de pouvoir communiquer avec vos amis via le système de messagerie ICQ, il faut créer une règle d'autorisation pour le flux UPD sortant. Ces paquets de données interviennent dans les requêtes DNS.

   Si vous souhaitez interdire l'affichage de diverses bannières ou l'apparition de fenêtres pop up pendant l'utilisation d'ICQ, vous devrez créer une règle pour l'application afin d'interdire l'activité TCP entrante et sortante (vous pouvez également utiliser Anti-Escroc pour une action similaire, pour de plus amples informations, consultez le Chapitre 11 à la page 141).

Si vous avez défini des paramètres de connexion au réseau (adresse, port, heure d'exécution), vous devrez également donner des valeurs précises.

Une fois que la règle aura été ajoutée à la liste des règles pour l'application, vous pourrez procéder à une configuration complémentaire (cf. ill. 46). Si vous souhaitez que la règle soit appliquée à l'application lancée avec des paramètres définis via la ligne de commande, cochez la case ☑ **Ligne de commande** et saisissez la ligne dans le champ situé à droite. La règle ne sera pas appliquée aux programmes lancés avec une autre variable de la clé de commande.

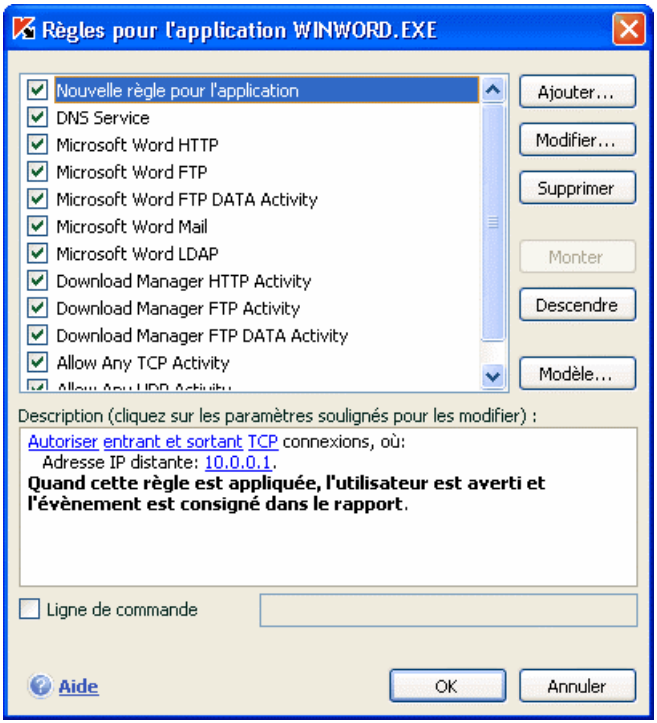


Illustration 46. Configuration complémentaire de la nouvelle règle

Il est possible également de créer une règle au départ de la boîte de dialogue de notification de la découverte d'une activité de réseau (cf. point 12.10, p. 175).

12.5. Modification de la priorité de la règle

Une priorité d'exécution est associée à chaque règle créée pour l'application. En diverses circonstances (par exemple, les paramètres de l'activité de réseau), une action sera exécutée sur l'activité de réseau de l'application. Cette action est définie par la règle dont la priorité est la plus élevée.

La priorité d'une règle dépend de sa position dans la liste des règles. La toute première règle de la liste est celle qui possède la priorité la plus élevée. Chaque règle créée manuellement est ajoutée en début de liste. Les règles créées sur la

base d'un modèle ou au départ d'une notification spéciale sont ajoutées à la fin de la liste.

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

1. Sélectionnez le nom de l'application dans l'onglet **Règles pour l'application** et cliquez sur **Modifier**.
2. A l'aide des boutons **Monter** et **Descendre** de la fenêtre contenant les règles créées, déplacez les règles vers le haut ou le bas de la liste afin de modifier de la sorte leur priorité.

Pour modifier la priorité de la règle pour le paquet, agissez de la manière suivante :

1. Sélectionnez la règle dans l'onglet **Règles pour les paquets**.
2. A l'aide des boutons **Monter** et **Descendre** de la fenêtre contenant les règles créées, déplacez les règles vers le haut ou le bas de la liste afin de modifier de la sorte leur priorité.

12.6. Règles pour les zones de sécurité

Une fois le programme installé, Anti-Hacker analyse le réseau dans lequel évolue l'ordinateur. Sur la base des résultats, le réseau est scindé en zones conventionnelles:

Internet, le réseau des réseaux. Dans cette zone, Kaspersky Internet Security fonctionne comme un pare-feu personnel. Toute l'activité de réseau est régie par les règles pour les paquets et les applications créées par défaut afin d'offrir une protection maximale. Vous ne pouvez pas modifier les conditions de la protection lorsque vous évoluez dans cette zone, si ce n'est activer le mode furtif de l'ordinateur afin de renforcer la protection.

Zones de sécurité, quelques zones conventionnelles qui correspondent souvent aux sous-réseaux auxquels votre ordinateur est connecté (il peut s'agir d'un sous-réseau local à la maison ou au bureau). Par défaut, ces zones sont considérées comme des zones à risque moyen. Vous pouvez modifier le statut de ces zones sur la base de la confiance accordée à un sous-réseau ou l'autre et configurer des règles pour les paquets et les applications.

Si le mode d'apprentissage d'Anti-Hacker est activé, chaque fois que l'ordinateur sera connecté à une nouvelle zone, une fenêtre s'affichera et présentera une brève description de ladite zone. Vous devrez attribuer un état à la zone, ce qui ultérieurement autorisera une activité de réseau quelconque:

- **Internet**. Cet état est attribué par défaut au réseau Internet car une fois qu'il y est connecté, l'ordinateur est exposé à tout type de menaces. Il est également conseillé de choisir cet état pour les réseaux qui ne sont protégés par aucun logiciel antivirus, pare-feu, filtre, etc. Cet état garantit la protection maximale de l'ordinateur dans cette zone, à savoir :
    - Le blocage de n'importe quelle activité de réseau NetBios dans le sous-réseau;
    - L'interdiction de l'exécution des règles pour les applications et les paquets qui autorisent l'activité de réseau NetBios dans le cadre de ce sous-réseau.

  Même si vous avez créé un dossier partagé, les informations qu'il contient ne seront pas accessibles aux utilisateurs d'un sous-réseau de ce type. De plus, lors de la sélection de cet état de réseau, vous ne pourrez pas accéder aux fichiers et aux imprimantes des autres ordinateurs du réseau.
- **Intranet**. Cet état est attribué par défaut à la majorité des zones de sécurité découvertes lors de l'analyse de l'environnement de réseau de l'ordinateur, à l'exception d'Internet. Il est conseillé de choisir cet état pour les zones qui représentent un risque moyen (par exemple, le réseau Interne d'une entreprise). En choisissant cet état, vous autorisez :
    - Toute activité de réseau NetBios dans le cadre du sous-réseau.
    - L'exécution des règles pour les applications et les paquets qui autorisent l'activité de réseau NetBios dans le cadre du sous-réseau donné.

  Sélectionnez cet état si vous souhaitez autoriser l'accès à certains répertoires de votre ordinateur et interdire toute autre activité externe. Les utilisateurs auront ainsi accès aux répertoires partagés, mais ils ne pourront pas exécuter un cheval de Troie.
- **De confiance**. Cet état doit être réservé uniquement aux zones qui, d'après vous, ne présentent aucun danger, c.-à-d. les zones où l'ordinateur ne sera pas exposé à des attaques ou à des tentatives d'accès non autorisé. Le choix de cet état implique l'autorisation de n'importe quelle activité de réseau. Même si vous avez sélectionné le niveau de protection maximale et que vous avez créé des règles d'interdiction, ces paramètres ne seront pas applicables aux ordinateurs distants de la zone de confiance.

N'oubliez pas que toute restriction relative à l'accès à un fichier ne fonctionne que dans le cadre du sous réseau indiqué.

Pour les réseaux dont l'état est **Intranet** ou **Internet**, vous pouvez activer le mode furtif pour plus de sécurité. Ce mode autorise uniquement l'activité initialisée par l'utilisateur ou une application autorisée. En d'autres termes, votre ordinateur devient "invisible" pour le monde extérieur. Vous pouvez toutefois continuer à utiliser Internet sans aucune difficulté.

Il n'est pas conseillé d'utiliser le mode furtif si l'ordinateur est utilisé en tant que serveur (ex. : serveur de messagerie ou serveur http). Si tel est le cas, les ordinateurs qui essaient de contacter ce serveur ne le verront pas dans le réseau.

La liste des zones dans lesquelles votre ordinateur est enregistré figure dans l'onglet **Réseau** (cf. ill. 47). Chaque zone est accompagnée de son état, d'une brève description du réseau et des informations relatives à l'utilisation ou non du mode furtif.

Pour modifier l'état d'une zone ou pour activer/désactiver le mode furtif, sélectionnez l'état dans la liste et cliquez sur les liens requis dans le bloc **Description** situé sous la liste. Vous pouvez réaliser les mêmes actions ainsi que modifier l'adresse et le masque du sous réseau dans la fenêtre **Paramètres du réseau** ouverte à l'aide du bouton **Modifier**.

Lors de la consultation de la liste des zones, vous pouvez en ajouter un nouveau, à l'aide du bouton **Chercher**. Anti-Hacker recherchera les réseaux enregistrables et, s'il en trouve, il vous propose d'en définir l'état. De plus, il est possible d'ajouter une nouvelle zone à la liste manuellement (par exemple, si vous raccordez votre ordinateur portable à un nouveau réseau). Pour ce faire, cliquez sur **Ajouter** et saisissez les informations requises dans la fenêtre **Paramètres de la zone**.

Afin de supprimer un réseau de la liste, cliquez sur **Supprimer**.

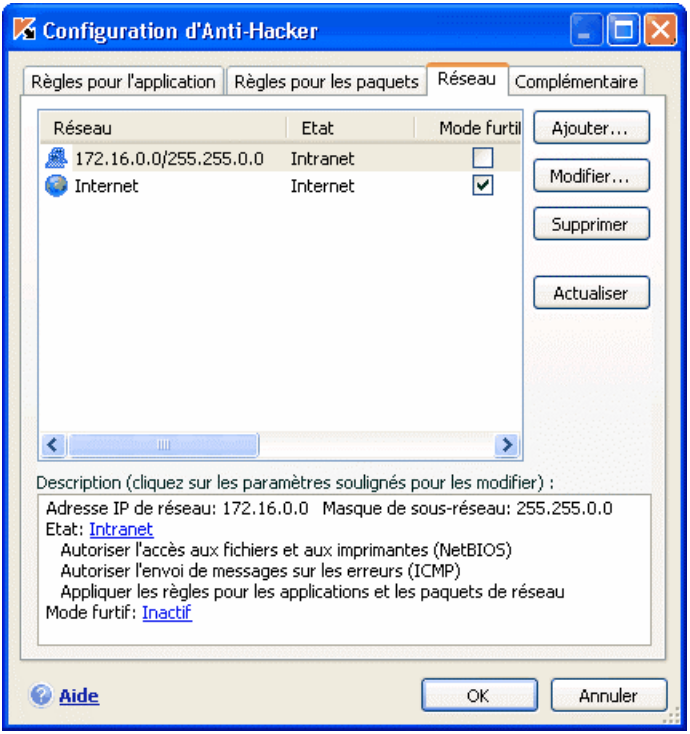


Illustration 47. Liste des règles pour le réseau

12.7. Mode de fonctionnement du pare-feu

Le mode de fonctionnement du pare-feu (cf. ill.) définit la compatibilité d'Anti-Hacker avec les programmes qui établissent de nombreuses connexions de réseau ainsi qu'avec les jeux en réseau.

Compatibilité maximale : mode de fonctionnement du pare-feu qui garantit le fonctionnement optimum d'Anti-Hacker et des programmes qui établissent de nombreuses connexions de réseau (clients des réseaux d'échange de fichiers). Toutefois, l'utilisation de ce mode peut ralentir dans certains cas la réaction dans les jeux de réseau. Si cela se produit, il est conseillé de choisir le mode Vitesse maximale.

Vitesse maximale : mode de fonctionnement du pare-feu qui garantit la réaction la plus rapide dans les jeux de réseau. Toutefois, ce mode peut entraîner

des conflits avec les clients des réseaux d'échange de fichiers ou d'autres applications de réseau. Dans ce cas, il est conseillé de désactiver le mode furtif.

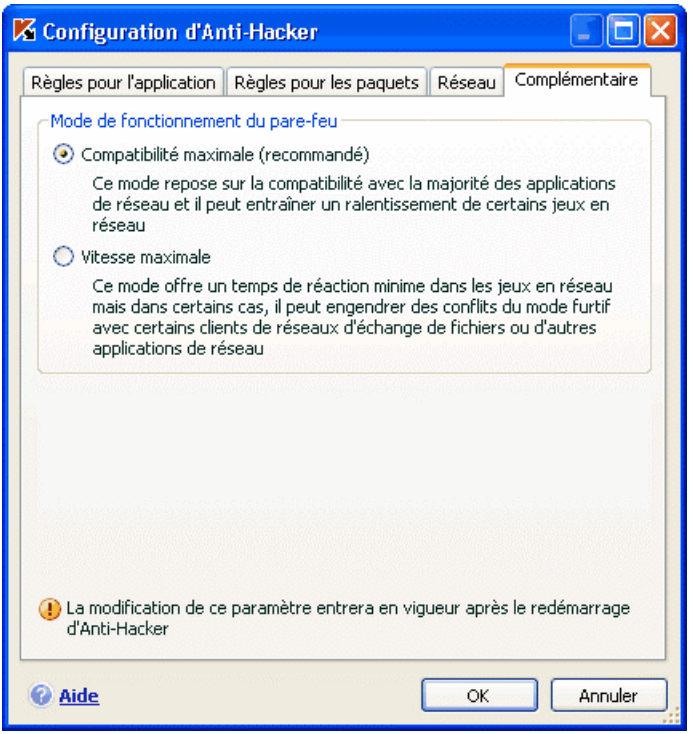


Illustration 48. Sélection du mode de fonctionnement d'Anti-Hacker

Pour configurer le mode de fonctionnement du pare-feu :

1. Cliquez sur **Configuration** dans la section Pare-feu de la boîte de dialogue de configuration d'Anti-Hacker.
2. Dans la fenêtre qui s'ouvre, passez à l'onglet **Complémentaire** et sélectionnez le mode voulu : Vitesse maximale ou Compatibilité maximale.

La modification du mode de fonctionnement du pare-feu entre en vigueur uniquement après le redémarrage du composant Anti-Hacker .

12.8. Configuration du système de détection d'intrusions

Toutes les attaques de réseau connues à ce jour qui menacent votre ordinateur sont reprises dans les signatures de menaces. Le module **Détecteur d'attaques** du composant Anti-Hacker fonctionne sur la base de la liste de ces attaques. L'enrichissement de la liste des attaques découvertes par ce module se produit lors de la mise à jour des signatures (cf. Chapitre 15, p. 219).

Le Détecteur d'attaques surveille l'activité de réseau propre aux attaques de réseau et lors de la découverte d'une tentative d'attaque, il bloque tout type d'activité de réseau émanant de l'ordinateur à l'origine de l'attaque pendant une heure. Un message vous avertit qu'une attaque de réseau a été menée et vous fournit des informations relatives à l'ordinateur à l'origine de l'attaque.

Vous pouvez configurer le système de détection d'intrusions. Pour ce faire :

3. Ouvrez la fenêtre de configuration d'Anti-Hacker.
4. Cliquez sur **Configuration** dans la section **Système de détection des intrusions**.
5. Dans la fenêtre qui s'ouvre (cf. ill. 49), définissez la nécessité de bloquer l'ordinateur à l'origine de l'attaque et pour combien de temps. Par défaut, l'ordinateur est bloqué pour 60 minutes. Vous pouvez réduire ou augmenter ce laps de temps en modifiant la valeur du champ situé à côté de la case **Bloquer l'ordinateur attaquant pendant… min**. Si vous ne voulez pas bloquer l'activité de réseau de l'ordinateur à l'origine de l'attaque, désélectionnez la case.

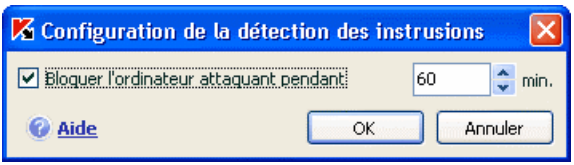


Illustration 49. Configuration du blocage temporaire de l'ordinateur attaquant

12.9. Liste des attaques de réseau découvertes

Il existe actuellement une grande diversité d'attaques de réseau qui exploitent aussi bien les failles des systèmes d'exploitation ou celles d'applications système

ou autre. Les malfaiteurs perfectionnent en continu leurs méthodes pour voler des informations confidentielles, mettre des systèmes hors service ou procéder au détournement total de l'utilisation de la machine dans le cadre d'un réseau de zombies pour mener de nouvelles attaques.

Afin de garantir la protection de l'ordinateur en permanence, il est bon de connaître les menaces qui planent sur ce dernier. Les attaques de réseau connues peuvent être scindées en trois grands groupes:

- **Balayage des ports** : ce type de menace n'est pas une attaque en tant que telle. En fait, c'est une activité qui, en général, précède l'attaque car il s'agit de l'un des principaux moyens existant pour obtenir des informations sur un ordinateur distant. Il s'agit de balayer les ports UDP/TCP utilisés par les services de réseau sur le nœud convoité afin de définir leur état (ouvert ou fermé).

  Le balayage des ports permet de comprendre quels sont les attaques qui peuvent réussir sur ce système. De plus, les informations obtenues suite au balayage donnent au malfaiteur une idée du système d'exploitation utilisé sur l'ordinateur distant. Et cela réduit encore plus le nombre d'attaques potentielles et par conséquent, le gaspillage de temps à organiser des attaques vouées à l'échec. Ces informations permettent également d'exploiter une vulnérabilité spécifique à ce système d'exploitation en question.

- **Attaque DoS ou attaque par déni de service** : ces attaques plongent le système victime dans un état instable ou non opérationnel. De tels attaques peuvent nuire aux ressources de données cibles ou les détruire, ce qui les rend inexploitables.

  Il existe deux types principaux d'attaques DoS :

  - envoi vers la victime de paquets spécialement formés et que l'ordinateur n'attend pas. Cela entraîne une surcharge ou un arrêt du système;
  - envoi vers la victime d'un nombre élevé de paquets par unité de temps; l'ordinateur est incapable de les traiter, ce qui épuise les ressources du système.

  Voici des exemples frappants de ce groupe d'attaques :

  - *Ping of death :* envoi d'un paquet ICMP dont la taille dépasse la valeur admise de 64 Ko. Cette attaque peut entraîner une panne dans certains systèmes d'exploitation.
  - L'attaque *Land* consiste à envoyer vers le port ouvert de votre ordinateur une requête de connexion avec lui-même. Suite à cette attaque, l'ordinateur entre dans une boucle, ce qui

augmente sensiblement la charge du processeur et entraîne une panne éventuelle du système d'exploitation.

- L'attaque *ICMP Flood* consiste à envoyer vers l'ordinateur de l'utilisateur un grand nombre de paquets ICMP. Cette attaque fait que l'ordinateur est obligé de répondre à chaque nouveau paquet, ce qui entraîne une surcharge considérable du processeur.

- L'attaque *SYN Flood* consiste à envoyer vers votre ordinateur un nombre élevé de requêtes pour l'ouverture d'une connexion. Le système réserve des ressources définies pour chacune de ces connexion. Finalement, l'ordinateur gaspille toutes ses ressources et cesse de réagir aux autres tentatives de connexion.

- **Attaques d'intrusion** qui visent à s'emparer du système. Il s'agit du type d'attaque le plus dangereux car en cas de réussite, le système passe entièrement aux mains du malfaiteur.

  Ce type d'attaque est utilisé lorsqu'il est indispensable d'obtenir des informations confidentielles sur l'ordinateur distant (par exemple, numéro de carte de crédit, mots de passe) ou simplement pour s'introduire dans le système en vue d'utiliser ultérieurement les ressources au profit du malfaiteur (utilisation du système dans un réseau de zombies ou comme base pour de nouvelles attaques).

  Ce groupe est également le plus important au vu du nombre d'attaques qu'il contient. Elles peuvent être réparties en trois sous-groupe en fonction du système d'exploitation : attaques sous Microsoft Windows, attaques sous Unix et un groupe commun pour les services de réseau utilisant les deux systèmes d'exploitation.

  Les attaques les plus répandues qui utilisent les services de réseau du système d'exploitation sont :

  - *les attaques de débordement du tampon* : type de vulnérabilité dans un logiciel qui résulte de l'absence de contrôle (ou de contrôle insuffisant) lors de la manipulation de données massives. Il s'agit de l'une des vulnérabilités les plus anciennes et des plus faciles à exploiter.

  - les attaques qui reposent sur des erreurs dans les chaînes de format : type de vulnérabilités dans les applications qui résultent d'un contrôle insuffisant des valeurs des paramètres de la fonction d'entrée/de sortie de format de type printf(), fprintf(), scanf() ou autres de la bibliothèque standard du langage C. Lorsqu'une telle vulnérabilité est présente dans un logiciel, le

malfaiteur, qui peut envoyer des requêtes formulées spécialement, peut prendre le contrôle complet du système.

Le détecteur d'attaque analyse automatiquement l'utilisation de telles vulnérabilité et les bloque dans les services de réseau les plus répandus (FTP, POP3, IMAP), s'ils fonctionnent sur l'ordinateur de l'utilisateur.

Les attaques sur le système d'exploitation Windows repose sur l'utilisation de vulnérabilités d'applications installées sur l'ordinateur (par exemple, Microsoft SQL Server, Microsoft Internet Explorer, Messenger ou les composants système accessibles via le réseau comme Dcom, SMB, Winds, LSASS, IIS5).

Par exemple, le composant Anti-Hacker protège l'ordinateur contre les attaques qui utilisent les vulnérabilités suivantes bien connue du logiciel (la liste des vulnérabilités reprend la numérotation conforme à la Microsoft Knowledge Base) :

(**MS03-026**) DCOM RPC Vulnerability(Lovesan worm)

(**MS03-043**) Microsoft Messenger Service Buffer Overrun

(**MS03-051**) Microsoft Office Frontpage 2000 Server Extensions Buffer Overflow

(**MS04-007**) Microsoft Windows ASN.1 Vulnerability

(**MS04-031**) Microsoft NetDDE Service Unauthenticated Remote Buffer Overflow

(**MS04-032**) Microsoft Windows XP Metafile (.emf) Heap Overflow

(**MS05-011**) Microsoft Windows SMB Client Transaction Response Handling

(**MS05-017**) Microsoft Windows Message Queuing Buffer Overflow Vulnerability

(**MS05-039**) Microsoft Windows Plug-and-Play Service Remote Overflow

(**MS04-045**) Microsoft Windows Internet Naming Service (WINS) Remote Heap Overflow

(**MS05-051**) Microsoft Windows Distributed Transaction Coordinator Memory Modification

De plus, dans certains cas, les attaques d'intrusion exploitent divers types de scripts malveillants, y compris des scripts traités par Microsoft Internet Explorer et diverses versions du ver Helkern. L'attaque *Helkern* consiste à envoyer vers l'ordinateur distant des paquets UDP d'un certain type capable d'exécuter du code malveillant.

N'oubliez pas que tout ordinateur connecté à un réseau est exposé chaque jour au risque d'attaque par une personne mal intentionnée. Afin de garantir la protection de votre ordinateur, vous devez absolument activer Anti-Hacker si vous vous connectez à Internet et mettre à jour régulièrement les signatures des attaques de pirates informatiques (cf. point 15.3.2, p. 225).

12.10. Autorisation / interdiction de l'activité de réseau

Si vous avez sélectionné le **Mode d'apprentissage** en tant que niveau de protection, un message spécial (cf. illustration) apparaîtra chaque fois qu'une tentative de connexion de réseau pour laquelle aucune règle n'existe est réalisée.

Par exemple, si vous utilisez Microsoft Office Outlook en tant que client de messagerie, votre courrier est téléchargé depuis le serveur Exchange une fois que le client de messagerie a été lancé. Afin de remplir votre boîte aux lettres, le logiciel établit une connexion de réseau avec le serveur de messagerie. Anti-Hacker va surveiller cette activité. Dans ce cas, un message (cf. ill. 50) reprenant les informations suivantes sera affiché :

- *Description de l'activité* : nom de l'application et brèves caractéristiques de la connexion qu'elle tente d'établir. Sont également indiqués : le type de connexion, le port local à partir de laquelle elle est établie, le port distant et l'adresse de la connexion. Pour obtenir de plus amples informations sur l'activité de réseau, cliquez avec le bouton gauche de la souris dans n'importe quel endroit du bloc. La fenêtre qui s'ouvre contient des informations sur la connexion, sur le processus qu'elle lance et sur l'éditeur de l'application.
- *Action* : la séquence d'opérations que doit exécuter Anti-Hacker par rapport à l'activité de réseau découverte. C'est cet aspect que vous devez définir vous-même.

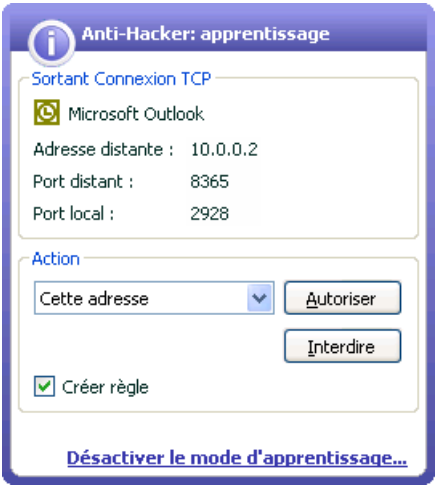


Illustration 50. Notification d'une activité de réseau

Etudiez attentivement les informations relatives à l'activité de réseau avant de choisir l'action d'Anti-Hacker. Il est conseillé de suivre ces recommandations lors de la prise de décision :

1. Décidez avant tout si vous voulez autoriser ou non l'activité de réseau. Peut-être que dans ce cas vous pourrez compter sur la sélection de règles déjà créées pour l'application ou le paquet en question (si elles ont été créées). Pour ce faire, cliquez sur **Sélection des règles**. Cette action entraîne l'ouverture d'une fenêtre dans laquelle figure la liste complète des règles créées pour l'application ou le paquet de données.
2. Définissez ensuite si l'action sera exécutée une seule fois ou automatiquement à chaque fois que ce type d'activité sera découvert.

Pour une exécution ponctuelle de l'action :

désélectionner la case **Créer règle** et cliquez sur le bouton portant le nom de l'action, par exemple **Autoriser**.

Pour que l'action que vous avez sélectionnée soit exécutée automatiquement chaque fois qu'une telle activité sera lancée sur l'ordinateur :

1. Cochez la case **Créer règle**.
2. Sélectionnez le type d'activité auquel vous souhaitez appliquer l'action parmi les propositions du menu déroulant du bloc **Action** :
   - **N'importe quelle activité** : n'importe quelle activité de réseau lancée par cette application.

- **Personnaliser** : activité particulière que vous devez définir dans une fenêtre spéciale identique à la fenêtre de création de règle.(cf. point 12.2.1, p. 157).
- **<Modèle>** : nom du modèle inclus dans la sélection de règles caractéristiques pour l'activité de réseau de l'application. Ce type d'activité apparaît dans la liste lorsqu'il existe pour l'application à l'origine de l'activité de réseau un modèle adéquat livré avec Kaspersky Internet Security (cf. point 12.2.2, p. 158). Dans ce cas, vous n'aurez pas à personnaliser l'activité à autoriser ou à interdire à ce moment. Utilisez le modèle et la sélection de règles pour l'application sera créée automatiquement.

3. Cliquez sur le bouton portant le nom de l'action (**Autoriser** ou **Interdire**).

N'oubliez pas que la règle créée sera utilisée uniquement lorsque tous les paramètres de la connexion seront conformes à la règle. Ainsi, la règle sera caduque en cas de connexion établie depuis un autre port local.

CHAPITRE 13. PROTECTION CONTRE LE COURRIER INDESIRABLE

Kaspersky Internet Security 2006 contient un composant spécial capable d'identifier le courrier indésirable et de le traiter conformément aux règles de votre client de messagerie, ce qui économise votre temps lors de l'utilisation du courrier électronique.

La recherche du courrier indésirable s'opère selon l'algorithme suivant :

1. Le composant vérifie si l'adresse de l'expéditeur figure dans la liste "noire ou la liste "blanche" des expéditeurs.
    - Si l'adresse de l'expéditeur figure dans la liste "blanche", le message reçoit le statut *courrier normal*.
    - Si l'adresse de l'expéditeur figure dans la liste "blanche", le message reçoit le statut *courrier indésirable*. Le traitement ultérieur du message dépendra de l'action que vous aurez choisie (cf. point 13.3.8, p. 197).
2. Si l'adresse de l'expéditeur ne figure ni dans la liste "noire, ni dans la liste "blanche", Anti-Spam analyse minutieusement le message à l'aide de la technologie PDB (cf. point 13.3.2, p. 187) et vérifie s'il contient des expressions caractéristiques du courrier indésirable. L'analyse repose sur l'utilisation de bases créées pendant l'entraînement d'Anti-Spam.
3. Anti-Spam analyse minutieusement le contenu du message et vérifie s'il contient des expressions reprises dans les listes "noire" ou "blanche".
    - Si le texte contient des expressions issues de la liste "blanche", le message reçoit le statut *courrier normal*.
    - Si le texte contient des expressions de la liste "noire", le message reçoit le statut *courrier indésirable*. Le traitement ultérieur du message dépendra de action que vous aurez choisie.
4. Si le message ne contient pas d'expressions reprises dans la liste "noire" ou "blanche", le composant recherche toute trace de phishing. Si le texte contient une adresse reprise dans la base de données anti-phishing, le message reçoit le statut *courrier indésirable*. Le traitement ultérieur du message dépendra de l'action que vous aurez choisie.

5. Si le message ne contient aucune expression de phishing, il est soumis à la détection du courrier indésirable à l'aide de l'une des trois technologies suivantes :
    - Analyse des images selon la technologie GSG;
    - Analyse du texte des messages à l'aide d'un algorithme d'identification du courrier indésirable, l'algorithme de Bayes.
6. Vient ensuite l'analyse des caractères complémentaires de filtrage du courrier indésirable (cf. point 13.3.5, p. 194), définis par l'utilisateur lors de la configuration d'Anti-Spam, par exemple l'analyse de l'exactitude des balises HTML, la taille des polices ou les caractères invisibles.

Vous avez la possibilité de désactiver chacune des étapes de recherche du courrier indésirable.

Anti-Spam se présente sous la forme d'un plug-in dans les clients de messagerie suivants :

- Microsoft Office Outlook (cf. point 13.3.9, p. 198);
- Microsoft Outlook Express (cf. point 13.3.10, p. 202);
- The Bat! (cf. point 13.3.11, p. 203).

La barre des tâches de Microsoft Office Outlook et Microsoft Outlook Express affiche les boutons **Courrier normal** et **Courrier indésirable**. Ceux-ci vous permettent d'entraîner Anti-Spam à reconnaître le courrier indésirable dans le contexte de chaque message. Ces boutons n'existent pas dans The Bat!, toutefois, il est possible d'entraîner ce client de messagerie à l'aide des éléments **Marquer comme courrier indésirable** et **Marquer comme courrier normal** dans le menu **Spécial**. En plus de tous les paramètres du client de messagerie, on retrouve des paramètres de traitement spécial du courrier indésirable (cf. point 13.3.1, p. 186).

Anti-Spam utilise une modification de l'algorithme d'apprentissage automatique (algorithme de Bayez) qui permet au composant d'établir une distinction plus précise entre *courrier indésirable* et *courrier normal*. Les spécialistes de Kaspersky Lab ont considérablement modifié l'algorithme de Bayes pour permettre une plus grande souplesse dans l'identification du courrier non désirable. Le contenu du message constitue la source de données pour l'algorithme de Bayes.

Il arrive parfois que l'algorithme modifié d'apprentissage automatique ne soit pas en mesure de décider avec certitude si un message appartient ou non au courrier indésirable. Un tel message reçoit le statut *courrier indésirable potentiel*.

Pour réduire le volume de messages classés comme courrier indésirable potentiel, il est conseillé de procéder à un entraînement d'Anti-Spam sur de tels messages (cf. point 13.2, p. 182). Pour ce faire, il est indispensable d'indiquer

les messages qui appartiennent au *courrier indésirable* et ceux qui appartiennent au *courrier normal*.

Les messages électroniques classés comme *courrier indésirable* ou *courrier indésirable potentiel* sont modifiés : Le texte **[!! SPAM]** ou **[?? Probable Spam]** est ajouté respectivement à l'**objet** du message.

Les règles de traitement des messages classés comme courrier indésirable ou courrier indésirable potentiel dans Microsoft Outlook, Microsoft Outlook Express et The Bat! sont définies au départ de plug-ins spéciaux créés pour ces clients. Pour les autres clients de messagerie, il est possible de créer des règles sur la base du contenu du champ **Objet** afin de rediriger les messages vers différents dossier si ce champ contient le texte **[!! SPAM]** ou **[?? Probable Spam]**. Pour obtenir de plus amples informations sur la création de règles de tri, consultez la documentation de votre client de messagerie.

13.1. Sélection du niveau d'agressivité d'Anti-Spam

Kaspersky Internet Security assure la protection contre le courrier indésirable selon un des 5 niveaux suivants (cf. ill. 51):

Tout bloquer. Niveau le plus élevé qui considère tous les messages comme courrier indésirable à l'exception de ceux contenant des expressions de la liste "blanche" (cf. point 13.3.4.1, p. 190) et dont l'expéditeur figure dans la liste "blanche". A ce niveau, l'analyse du courrier s'effectue uniquement sur la base de la liste blanche, les autres technologies étant désactivées.

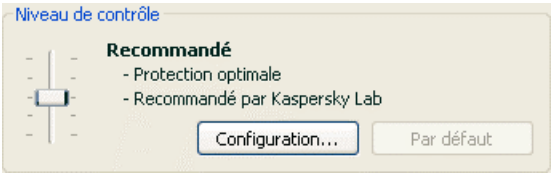


Illustration 51. Sélection du niveau de protection contre le courrier indésirable

Elevé – Niveau plus élevé qui entraînera peut-être la classification en tant que courrier indésirable de messages qui sont en fait des messages normaux. L'analyse des messages s'opèrent selon les listes "blanches" et "noires" et à l'aide des technologies PDB et GSG et de l'algorithme de Bayez (cf. point 13.3.2, p. 187).

Ce mode doit être utilisé lorsqu'il est fort probable que l'adresse du destinataire est inconnue des spammeurs. Par exemple, lorsque le destinataire n'est pas abonné à des listes de diffusion et qu'il ne possède

pas de boîtes aux lettres dans un service de messagerie électronique gratuit.

Recommandé : il s'agit de la configuration la plus universelle du point de vue de la classification des messages électroniques.

Dans ce mode, il se peut que du courrier indésirable ne soit pas reconnu comme tel et que des messages normaux soient classés comme courrier indésirable. Cela signifie que l'entraînement d'Anti-Spam n'est pas suffisant. Il est recommandé d'affiner l'entraînement à l'aide de l'Assistant d'apprentissage (cf. point 13.2.1, p. 182) ou des boutons **Courrier indésirable/Courrier normal** (ou des points du menu dans The Bat!) sur les messages qui n'ont pas été correctement identifiés.

Faible : il s'agit de la configuration la plus fidèle. Elle est recommandée aux utilisateurs dont le courrier entrant contient beaucoup de mots propres, selon Anti-Spam, au courrier indésirable alors qu'il s'agit de courrier normal. Cette situation se présente lorsque l'utilisateur, dans le cadre de ses activités professionnelles, est amené à utiliser dans sa correspondance des termes professionnels que l'on retrouve souvent dans le courrier indésirable. Toutes les technologies d'identification du courrier indésirable interviennent à ce niveau.

Ignorer tout : il s'agit d'un niveau le plus faible. Sont considérés comme courrier indésirable uniquement les messages qui contiennent des expressions extraites de la liste "noire" et dont l'expéditeur figure dans la liste "noire". A ce niveau, l'analyse du courrier s'effectue uniquement sur la base de la liste "noire", les autres technologies étant désactivées.

Par défaut, la protection contre le courrier indésirable s'opère selon les paramètres du niveau **Recommandé**.

Vous pouvez augmenter ou réduire le niveau ou modifier les paramètres du niveau actuel.

Pour modifier le niveau :

Déplacez simplement le curseur sur l'échelle d'agressivité. En définissant le niveau d'agressivité, vous pouvez définir le rapport des facteurs de courrier indésirable, du courrier indésirable potentiel et du courrier utile (cf. point 13.3.3, p. 188).

Pour modifier les paramètres du niveau actuel :

cliquez sur **Configuration** dans la fenêtre des paramètres d'Anti-Spam, modifiez les paramètres selon vos besoins et cliquez sur **OK**.

Suite à cette action, le niveau de protection devient **Utilisateur** qui correspond à la configuration que vous avez définie.

13.2. Entraînement d'Anti-Spam

Anti-Spam est livré avec une base de messages qui comprend 50 exemples de messages non sollicités. Il est conseillé d'entraîner Anti-Spam à reconnaître le courrier indésirable sur la base des messages que vous recevez.

Il existe plusieurs approches pour entraîner Anti-Spam :

- Utilisation de l'Assistant d'apprentissage (apprentissage groupé) (cf. point 13.2.1, p. 182).
- Apprentissage sur les messages sortant (cf. point 13.2.2, p. 183).
- Entraînement indirect pendant le travail avec le courrier électronique à l'aide des boutons spéciaux dans la barre d'outils du client de messagerie ou des points du menu (cf. point 13.2.3, p. 184).
- Entraînement lors de l'utilisation des rapports d'Anti-Spam (cf. point 13.2.4, p. 184).

L'entraînement à l'aide de l'Assistant d'apprentissage est préférable au tout début de l'utilisation d'Anti-Spam. L'Assistant permet d'entraîner Anti-Spam sur une grande quantité de messages électroniques.

N'oubliez pas que la quantité de messages pour l'entraînement au départ d'un dossier ne peut pas dépasser 50. Si le dossier compte plus de messages, l'entraînement sera réalisé sur la base de 50 messages uniquement.

Il est préférable de procéder à l'entraînement complémentaire à l'aide des boutons de l'interface du client du messagerie pendant l'utilisation directe du courrier électronique.

13.2.1. Assistant d'apprentissage

L'Assistant d'apprentissage permet d'entraîner Anti-Spam par paquet en précisant les dossiers de la boîte aux lettres qui contiennent le courrier indésirable et ceux qui contiennent le courrier normal.

Pour lancer l'Assistant d'apprentissage :

1. Sélectionnez **Anti-Spam** dans la fenêtre de configuration.
2. Cliquez sur **Assistant d'apprentissage** dans la partie droite de la fenêtre

L'Assistant d'apprentissage entraîne Anti-Spam étape par étape. Pour passer à l'étape suivante, cliquez sur **Suivant** et pour revenir à l'étape précédente, cliquez sur **Précédent**.

La première étape correspond à la sélection du dossier contenant le courrier normal. Vous devrez sélectionnez uniquement les dossiers dont vous êtes certain du contenu.

La deuxième étape correspond à la sélection du dossier contenant le courrier indésirable.

La troisième étape correspond à l'apprentissage automatique d'Anti-Spam sur la base des dossiers que vous avez sélectionnés. Les messages de ces dossiers viennent s'ajouter à la base d'Anti-Spam. Les expéditeurs du courrier normal sont repris automatiquement dans la liste "blanche".

La quatrième étape correspond à la sauvegarde des résultats de l'entraînement de l'une des manières suivantes : ajouter les résultats à la base existante ou remplacer la base existante par les résultats de l'entraînement. N'oubliez pas que pour assurer une identification efficace du courrier indésirable, il est indispensable de réaliser l'entraînement sur un minimum de 50 exemplaires de courrier normal et de 50 exemplaires de courrier indésirable. L'algorithme de Bayes ne pourra fonctionner sans cela.

Afin de gagner du temps, l'Assistant réalisera l'entraînement uniquement sur 50 messages de chaque dossier sélectionné.

13.2.2. Entraînement sur le courrier sortant

Vous pouvez réaliser l'entraînement d'Anti-Spam sur la base du courrier sortant de votre client de messagerie. Dans ce cas, la liste "blanche" des adresses sera enrichie sur la base des destinataires des messages sortant. L'apprentissage utilise uniquement les 50 premiers messages sortants, après quoi il arrête.

Pour activer l'entraînement d'Anti-Spam sur la base du courrier sortant:

1. Sélectionnez **Anti-Spam** dans la boîte de dialogue de configuration
2. Cochez la case ☑ **Sur la base du courrier sortant** dans la section **Apprentissage**.

Attention !

L'entraînement d'Anti-Spam sur le courrier sortant envoyé via le protocole MAPI a lieu uniquement lorsque la case ☑ **Analyser à l'envoi** du plug-in de l'antivirus de courrier électronique pour Microsoft Office Outlook a été cochée (cf. point 13.3.9, p. 198).

13.2.3. Entraînement à l'aide de votre client de messagerie électronique

L'entraînement pendant l'utilisation du courrier électronique suppose l'utilisation des boutons spéciaux situés dans la barre d'outils de votre client de messagerie.

Lors de l'installation, Anti-Spam s'intègre aux clients de messagerie suivants :

- Microsoft Office Outlook.
- Microsoft Outlook Express
- The Bat!

Les boutons **Courrier indésirable** et **Courrier normal** apparaissent dans le barre d'outils du Microsoft Office Outlook ainsi que l'onglet Anti-Spam avec les actions dans le menu **Service → Paramètres** (cf. point 13.3.9, p. 198).. Dans Microsoft Outlook Express, en plus des boutons **Courrier indésirable** et **Courrier normal**, on trouve également le bouton **Configuration** dans la barre des tâches. Ce bouton ouvre la fenêtre des actions à réaliser sur le courrier indésirable (cf. point 13.3.10, p. 202). Ces boutons n'existent pas dans The Bat!, toutefois, il est possible d'entraîner ce client de messagerie à l'aide des éléments **Marquer comme courrier indésirable** et **Marquer comme courrier normal** dans le menu **Spécial**.

Si vous estimez que le message sélectionné est un exemple de courrier indésirable, cliquez sur **Courrier indésirable**. Si ce message n'est pas un exemple de courrier indésirable, cliquez sur **Courrier normal**. Anti-Spam sera entraîné sur la base du message sélectionné. Si vous sélectionnez plusieurs messages, l'entraînement aura lieu sur la base de tous les messages sélectionnés.

Attention !

Si vous êtes forcé de sélectionner directement plusieurs messages ou si vous êtes convaincus qu'un dossier ne contient des messages que d'une seule catégorie (courrier indésirable ou courrier normal), il est possible de réaliser un entraînement groupé à l'aide de l'Assistant d'apprentissage (cf. point 13.2.1, p. 182).

13.2.4. Entraînement à l'aide des rapports d'Anti-Spam

Il est possible d'entraîner Anti-Spam sur la base de ses rapports.

Pour consulter les rapports du composant :

1. Sélectionnez **Anti-Spam** dans la section **Protection** de la fenêtre principale du logiciel.
2. Réalisez un clique gauche dans le bloc **Statistiques**.

Les rapports du composant permettent de conclure de la précision de la configuration et, au besoin, d'introduire des modifications dans le fonctionnement d'Anti-Spam.

Pour désigner un message comme appartenant au courrier indésirable ou normal :

1. Sélectionnez-le dans la liste du rapport de l'onglet **Evénements** et cliquez sur **Actions**.
2. Sélectionnez l'un des éléments suivants (cf. ill. 52):
   - **Marquer comme courrier indésirable**
   - **Marquer comme courrier normal**.
   - **Ajouter à la liste "blanche"**
   - **Ajouter à la liste "noire"**

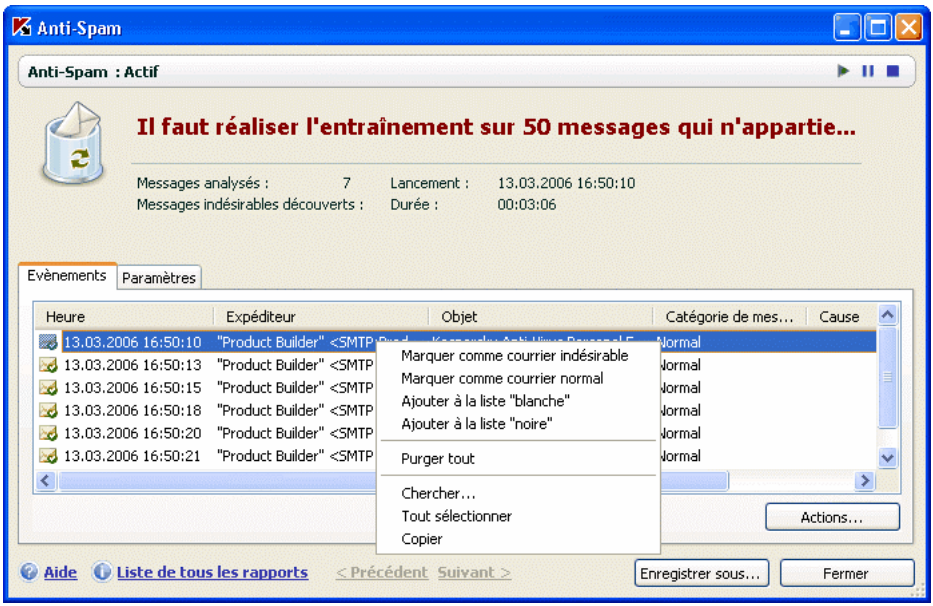


Illustration 52. Entraînement d'Anti-Spam au départ des rapports

L'entraînement d'Anti-Spam sera réalisé sur la base de ce message.

13.3. Configuration d'Anti-Spam

La configuration détaillée d'Anti-Spam est un attribut incontournable de la protection contre le courrier indésirable. Tous les paramètres du composant sont repris dans la fenêtre de configuration de Kaspersky Internet Security et vous permettent de :

- Définir les particularités du fonctionnement d'Anti-Spam (cf. point 13.3.1, p. 186).
- Choisir parmi les différentes technologies de filtrage du courrier indésirable (cf. point 13.3.2, p. 187).
- Régler l'exactitude de l'identification du courrier indésirable et du courrier normal (cf. point 13.3.3, p. 188).
- Composer des listes "noire" et "blanche" pour les expéditeurs et les expressions clé (cf. point 13.3.4, p. 189)
- Configurer critères complémentaires de filtrage du courrier indésirable (cf. point 13.3.5, p. 194).
- Réduire au maximum le volume de courrier indésirable dans votre boîte aux lettres grâce au dispatcher de messages (cf. point 13.3.7, p. 196).

Tous ces types de paramètres sont abordés en détails ci-après.

13.3.1. Configuration de l'analyse

Vous pouvez configurer les aspects suivants de l'analyse :

- Faut-il analyser le trafic de messagerie des protocoles POP3 et IMAP. Kaspersky Internet Security analyse par défaut le courrier de tous ces protocoles à l'exception des lettres cryptées via SSL.
- Faut-il activer les plug-ins pour Microsoft Office Outlook, Microsoft Outlook Express et TheBat!
- Faut-il consulter le courrier dans le dispatcher de messages (cf. point 13.3.7, p. 196).chaque fois avant de télécharger le courrier du serveur de messagerie dans la boîte de messagerie de l'utilisateur via le protocole POP3.

Pour configurer les paramètres cités ci-dessus :

1. Sélectionnez **Anti-Spam** dans la fenêtre de configuration de Kaspersky Internet Security.
2. Cochez les adéquates dans le bloc **Intégration au système** (cf. ill. 53).
3. Rectifiez, le cas échéant, les paramètres du réseau.

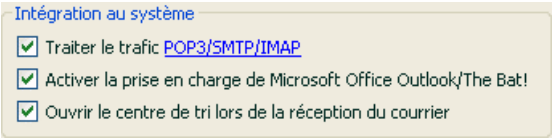


Illustration 53. Configuration des paramètres de l'analyse

13.3.2. Sélection de la technologie de filtrage du courrier indésirable

La recherche des messages non sollicités dans le courrier s'opère sur la base de technologies de filtrage modernes :

- **Technologie iBayes**, fondée sur le théorème de Bayes. Elle permet d'analyse le texte d'un message en recherchant dans son contenu les expressions caractéristiques du courrier indésirable. L'analyse repose sur les statistiques obtenues pendant l'entraînement d'Anti-Spam (cf. point 13.2, p. 182).
- **Technologie GSG**. Elle permet d'analyser les images des courriers électroniques à l'aide de signatures graphiques uniques capables d'identifier les messages non sollicités sous forme graphique.
- **Technologie PDB**. Elle permet d'analyser l'en-tête des messages électroniques et de les classer comme messages non sollicités sur la base d'un ensemble de règles heuristiques.

L'utilisation de toutes les technologies est activée par défaut, ce qui permet de réaliser le filtrage le plus complet du courrier.

Afin de désactiver l'application d'une technologie de filtrage particulière :

1. Ouvrez la boîte de dialogue de configuration d'Anti-Spam en cliquant sur Configuration dans la fenêtre principale du logiciel.
2. Cliquez sur **Configuration** dans le bloc **Niveau de contrôle** et dans la fenêtre qui s'ouvre, passez à l'onglet **Identification du courrier indésirable** (cf. ill. 54).

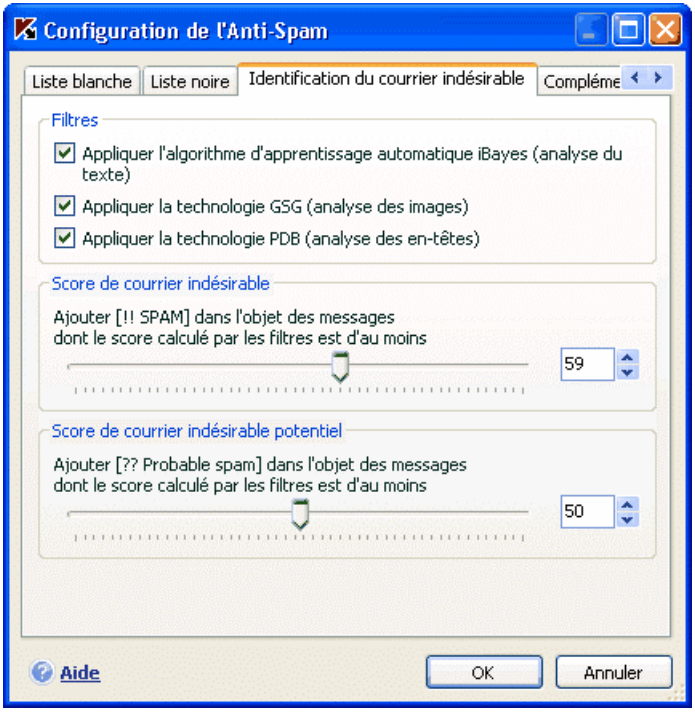


Illustration 54. Configuration de l'identification du courrier indésirable

3. Désélectionnez la case qui se trouve en regard de la technologie de filtrage que vous ne souhaitez pas utiliser lors de la recherche de courrier indésirable.

13.3.3. Définition des paramètres de courrier indésirable et de courrier indésirable potentiel

Les experts de Kaspersky Lab ont fait de leur mieux pour configurer Anti-Spam afin qu'il reconnaisse le courrier indésirable et le courrier indésirable potentiel.

L'identification du courrier indésirable repose sur l'utilisation de technologies modernes de filtrage (cf. point 13.3.2, p. 187) capables d'entraîner assez efficacement Anti-Spam sur la base d'un nombre défini de messages à reconnaître le courrier indésirable, le courrier indésirable potentiel et le courrier normal.

L'entraînement d'Anti-Spam est réalisé à l'aide de l'Assistant d'apprentissage ou via les clients de messagerie. Chaque élément de courrier normal ou de courrier indésirable se voit attribuer un certain coefficient. Quand un message arrive dans votre boîte aux lettres, Anti-Spam exploite la technologie iBayes pour voir si le message contient des éléments de courrier indésirable ou de courrier normal. Les coefficients de chaque élément de courrier indésirable (courrier normal) sont ajoutés pour obtenir le *facteur de courrier indésirable* et le *facteur de courrier indésirable potentiel*.

Le facteur de courrier indésirable potentiel définit la probabilité qu'à un message d'être un courrier indésirable potentiel. Si le niveau **Recommandé** est utilisé, tout message dont la probabilité est comprise entre 50 et 59% sera considéré comme *courrier indésirable potentiel*. Sera considéré comme appartenant au courrier normal tout message dont la probabilité sera inférieure à 50%.

Le facteur de courrier indésirable définit la probabilité qu'Anti-Spam considère un message comme exemple de courrier indésirable. Tout message dont la probabilité est supérieure à la valeur indiquée sera considéré comme appartenant au courrier indésirable. Par défaut, au niveau **Recommandé**, le facteur de courrier indésirable est égal à 59%. Cela signifie que n'importe quelle message dont la probabilité est supérieure à 59% sera considéré comme appartenant au courrier indésirable.

Il existe cinq niveaux d'agressivité (cf. point 13.1, p. 180) dont trois (**Elevé, Recommandé** et **Bas**) reposent sur diverses valeurs du facteur de courrier indésirable et le facteur de courrier indésirable potentiel.

Vous pouvez vous-même rectifier l'algorithme de fonctionnement d'Anti-Spam. Pour ce faire :

1. Sélectionnez **Anti-Spam** dans la fenêtre des paramètres de Kaspersky Internet Security.
2. Dans le bloc **Niveau de contrôle** de la partie droite de la fenêtre, cliquez sur **Configuration**.
3. Dans la fenêtre qui s'ouvre, modifiez les paramètres de courrier indésirable et de courrier indésirable potentiel dans les blocs du même nom de l'onglet **Identification du courrier indésirable** (cf. ill. 54).

13.3.4. Composition manuelle des listes "noire" et "blanche"

L'utilisateur compose les listes "noire" et "blanche" manuellement sur la base du fonctionnement d'Anti-Spam sur le courrier. Ces listes contiennent des informations relatives aux adresses de l'utilisateur, aux messages considérés

comme utiles ou indésirables ainsi qu'aux divers termes clés ou expressions qui permettent d'identifier un message comme étant utile ou non sollicité.

L'application principale de la liste des expressions clé, en particulier celle de la liste "blanche" consiste à convenir avec des expéditeurs définis (vos collègues par exemple) d'une signature quelconque pour les messages. Cette signature peut être n'importe quoi. Vous pouvez utilisez par exemple une signature PGP. Aussi bien dans la signature que dans les noms, il est possible d'utiliser des maques. * et **?**. Le caractère * représente n'importe quelle séquence de caractères de longueur aléatoire; le caractère **?** représente n'importe quel caractère unique.

Si les caractères * et **?** font partie d'une signature, il convient de les faire précéder du caractère \ afin d'éviter toute confusion de la part d'Anti-Spam. Dans ce cas, au lieu d'utiliser un caractère, on en utilise deux : *****et **\?**.

13.3.4.1. Liste "blanche" des adresses et des expressions

La liste "blanche" contient les expressions clé des messages que vous avez marqué comme courrier normal et les adresses des expéditeurs qui, selon vous, ne vous enverront jamais de courrier indésirable. La liste "blanche" des expressions est composée manuellement, tandis que la liste des expéditeurs est créée automatiquement pendant l'entraînement d'Anti-Spam. Vous pouvez modifier cette liste.

Pour passer à la configuration de la liste "blanche" :

1. Sélectionnez **Anti-Spam** dans la fenêtre de configuration de Kaspersky Internet Security.
2. Cliquez sur **Configuration** dans la partie droite de la fenêtre
3. Ouvrez l'onglet **Liste "blanche"** (cf. ill. 55).

L'onglet est scindé en deux blocs : le bloc supérieur reprend les adresses des expéditeurs de courrier normal tandis que le bloc inférieur affiche les expressions clé de ces messages.

Afin de recourir aux listes "blanche" des expressions et des adresses lors du filtrage du courrier, cochez les cases correspondantes dans les blocs **Expéditeurs autorisés** et **Expressions autorisées**.

Vous pouvez modifier la liste à l'aide des boutons de chaque bloc.

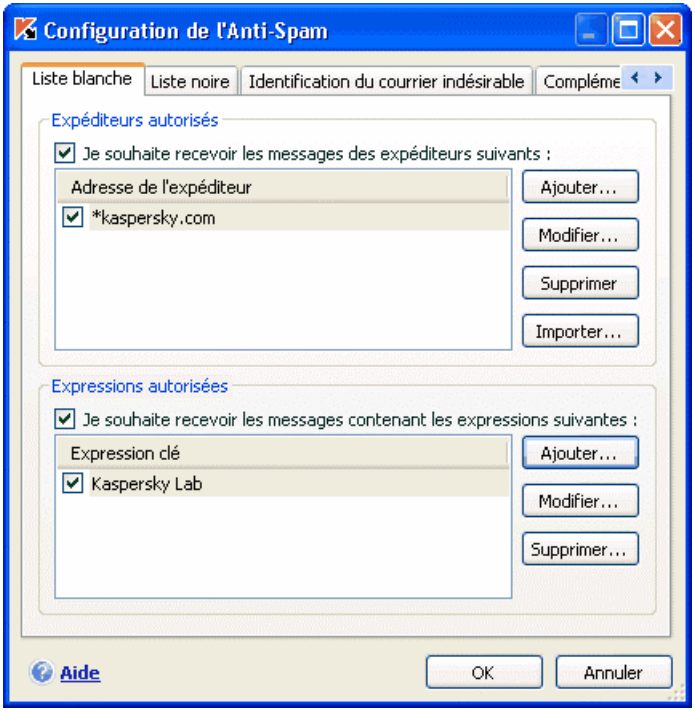


Illustration 55. Configuration de la liste "blanche" des adresses et des expressions

S'agissant des adresses de la liste, vous pouvez saisir soit une adresse, soit un masque. La case n'a pas d'importance lors de la saisie de l'adresse. voici quelques exemples de masques d'adresse :

dupont@test.fr : les messages de cet expéditeur seront considérés comme du courrier normal ;

**@test.fr* : les messages de n'importe quel expéditeur du domaine *test.fr* seront considérés comme du courrier normal ; exemple : *legrand@test.fr*, *dunant@test.fr*;

*dupont@** : les expéditeurs portant ce nom, quel que soit le domaine de messagerie, envoient toujours du courrier normal, par exemple : *dupont@test.fr*, *dupont@mail.fr*;

@test : les messages de n'importe quel expéditeur d'un domaine commençant par *test* n'appartiennent pas au courrier indésirable, par exemple : *dupont@test.fr*, *legrand@test.com;*

pierre.@test.???* le courrier dont le nom de l'expéditeur commence par *pierre,* dont le nom de domaine commence par *test* et se termine par une séquence quelconque de trois caractères sera toujours considéré comme du courrier normal; exemple : *pierre.dupont@test.com*, *pierre.legrand@test.org*.

Les masques peuvent être appliqués également aux expressions. La case n'a pas d'importance lors de la saisie de l'expression. Voici quelques exemples :

Salut Pierre ! Le message qui contient ce texte uniquement est considéré comme courrier normal. Il n'est pas conseillé d'utiliser ce genre d'expression dans la liste blanche.

*Salut Pierre !** : le message qui commence par cette ligne est considéré comme du courrier normal.

*Salut *! ** : le message qui débute par *Salut* et qui possède un point d'exclamation n'importe où dans le texte n'est pas considéré comme un courrier indésirable.

** Pierre? ** : le message adressé à *Pierre* suivi de n'importe quel caractère n'est pas considéré comme du courrier indésirable.

** Pierre\? ** : le message qui contient le texte *Pierre?* est considéré comme du courrier normal.

Si à un moment donné, vous souhaitez annuler la classification d'une adresse ou d'une expression quelconque en tant qu'attribut du courrier normal, vous devrez la supprimer de la liste en désélectionnant la case qui se trouve en regard.

Il est possible d'importer les adresses dans la liste "blanche" au départ d'un fichier CSV.

13.3.4.2. Liste "noire" des adresses et des expressions

La liste "noire" des expéditeurs contient les expressions clé des messages qui appartiennent au *courrier indésirable* ainsi que l'adresse des expéditeurs. La liste est rédigée manuellement.

Pour passer à la rédaction de la liste "noire" :

1. Sélectionnez **Anti-Spam** dans la fenêtre de configuration de Kaspersky Internet Security.
2. Cliquez sur **Configuration** dans la partie droite de la fenêtre
3. Ouvrez l'onglet **Liste "noire"** (cf. ill. 56).

L'onglet est scindé en deux blocs : le bloc supérieur reprend les adresses des expéditeurs de courrier indésirable tandis que le bloc inférieur affiche les expressions clé de ces messages.

Afin de recourir aux listes "noires" des expressions et des adresses lors du filtrage du courrier, cochez les cases correspondantes dans les blocs **Expéditeurs autorisés** et **Expressions autorisées**.

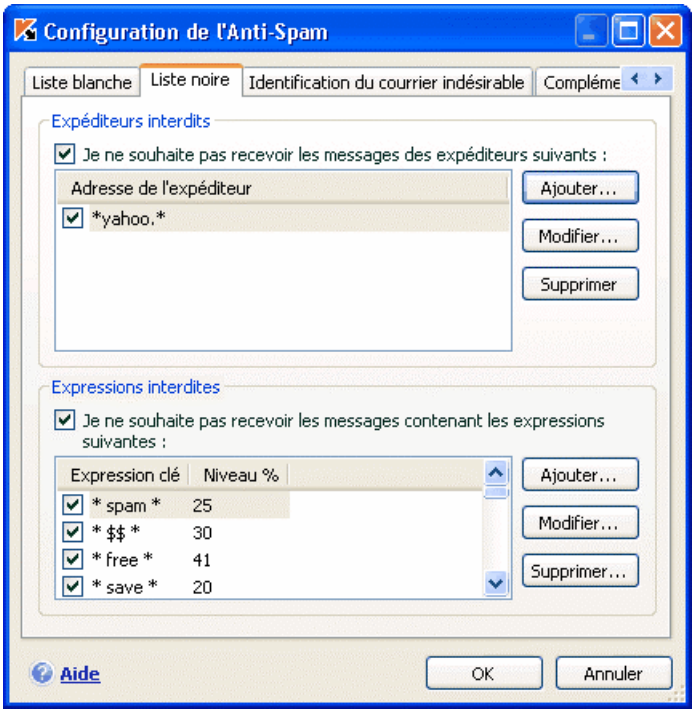


Illustration 56. Configuration de la liste "noire" des adresses et des expressions

Vous pouvez modifier la liste à l'aide des boutons de chaque bloc.

S'agissant des adresses de la liste, vous pouvez saisir soit une adresse, soit un masque. La case n'a pas d'importance lors de la saisie de l'adresse. Voici quelques exemples de masques d'adresse :

dupont@test.fr : les messages de cet expéditeur seront toujours considérés comme du courrier indésirable ;

**@test.fr* : les messages de n'importe quel expéditeur du domaine *test.fr* seront considérés comme du courrier indésirable ; exemple : *legrand@test.fr*, *dunant@test.fr*;

*dupont@** : les expéditeurs portant ce nom, quel que soit le domaine de messagerie, envoient toujours du courrier indésirable, par exemple : *dupont@test.fr*, *dupont@mail.fr*;

@test : les messages de n'importe quel expéditeur d'un domaine commençant par *test* appartiennent au courrier indésirable, par exemple : *dupont@test.fr*, *legrand@test.com;*

ivan.@test.???* le courrier dont le nom de l'expéditeur commence par *pierre et* dont le nom de domaine commence par *test* et se termine par une séquence quelconque de trois caractères sera toujours considéré comme du courrier indésirable; exemple : pierre.dupont@test.com, *pierre.legrand@test.org*.

Les masques peuvent être appliqués également aux expressions. La case n'a pas d'importance lors de la saisie de l'expression. Voici quelques exemples :

Salut Pierre ! Le message qui contient ce texte uniquement est considéré comme courrier indésirable. Il n'est pas conseillé d'utiliser ce genre d'expression dans la liste.

*Salut Pierre !** : le message qui commence par cette ligne est considéré comme du courrier indésirable.

*Salut *! ** : le message qui débute par *Salut* et qui possède un point d'exclamation n'importe où dans le texte est considéré comme un courrier indésirable.

** Pierre? ** : le message adressé à *Pierre* suivi de n'importe quel caractère est considéré comme du courrier indésirable.

** Pierre\? ** : le message qui contient le texte *Pierre?* est considéré comme du courrier indésirable.

Si à un moment donné, vous souhaitez annuler la classification d'une adresse ou d'une expression quelconque en tant qu'attribut du courrier indésirable, vous devrez la supprimer de la liste en désélectionnant la case qui se trouve en regard.

13.3.5. Signes complémentaires de filtrage du courrier indésirable

En plus des signes principaux utilisés pour le filtrage du courrier indésirable (constitution des listes "blanche" et "noire", recherche d'éléments de phishing, recherche à l'aide des technologies de filtrage), vous pouvez définir des signes complémentaires.

Afin de configurer les signes complémentaires pour le filtrage du courrier indésirable :

1. Sélectionnez **Anti-Spam** dans la fenêtre de configuration de Kaspersky Internet Security.
2. Cliquez sur **Configuration** dans la partie droite de la fenêtre.
3. Ouvrez l'onglet **Complémentaire** (cf. ill. 57).

Cet onglet reprend la liste des caractéristiques qui permettra d'attribuer le statut de *courrier indésirable* à un message avec plus ou moins de certitude.

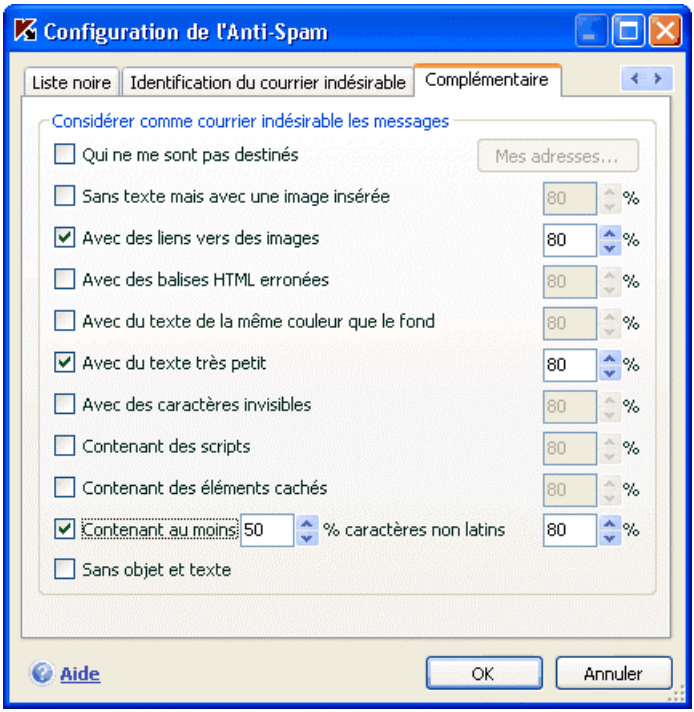


Illustration 57. Paramètres complémentaires d'identification du courrier indésirable

Afin d'activer l'utilisation d'une caractéristique quelconque, cochez la case située en regard de celle-ci. De plus, il faut définir pour chaque caractéristique le facteur de courrier indésirable (en pour cent) qui définit la probabilité avec laquelle un message sera considéré comme non sollicité. Par défaut, le facteur de courrier indésirable est de 80%. Les messages seront marqués comme *non sollicité* si la somme des probabilités pour l'ensemble des caractéristiques dépasse 100%.

Si vous activez le filtrage en fonction du paramètres "messages qui ne me sont pas adressé", vous devrez indiquer la liste de vos adresses dans la fenêtre qui s'ouvre à l'aide du bouton **Mes adresses**.

13.3.6. Constitution d'une liste d'adresses de confiance

Si vous activez le filtrage du courrier indésirable selon le critère "messages qui ne me sont pas adressés", vous devrez préciser vos adresses électroniques de confiance.

L'adresse du destinataire sera analysée lors de la recherche du courrier indésirable. Si l'adresse ne correspond à aucune des adresses de votre liste, le message sera considéré comme *non sollicité*.

La constitution et la modification de la liste des adresses s'opère dans la fenêtre **Mes adresses électroniques** à l'aide des boutons **Ajouter**, **Modifier** et **Supprimer**.

13.3.7. Dispatcher de messages

Attention !

Le Dispatcher de messages est disponible uniquement si vous recevez le courrier via le protocole POP3.

Le Dispatcher de messages est prévu pour l'examen des messages électroniques sur le serveur sans les télécharger sur votre ordinateur. Cela évite la réception de certains messages, ce qui vous fait gagner du temps et de l'argent lors de l'utilisation du courrier électronique et qui réduit la probabilité de recevoir du courrier indésirable et des virus.

Le Dispatcher de messages (cf. ill.) s'ouvre si la case **Ouvrir le centre de tri lors de la réception du courrier** a été cochée.

Pour supprimer un message sur le serveur sans avoir à le télécharger sur l'ordinateur :

cochez la case à gauche du message que vous souhaitez supprimer et cliquez sur **Supprimer**. Ce message sera supprimé du serveur. Le reste de la correspondance sera téléchargé sur l'ordinateur après la fermeture du Dispatcher.

Il est parfois difficile de décider de supprimer un message sur la seule base de l'expéditeur et de l'objet du message. Dans de telles situations, le Dispatcher de

messages vous propose des informations étendues sur le message en téléchargeant son en-tête.

Pour afficher l'en-tête du message :

Sélectionnez le message dans la liste du courrier entrant. Les en-têtes des messages seront affichées dans la partie inférieure du formulaire.

La taille des en-têtes est négligeable (quelques dizaines d'octets) et elles ne peuvent pas contenir de code malveillant.

L'examen des en-têtes peut être utile dans les cas suivants : les spammeurs ont installé un programme malveillant sur l'ordinateur de votre collègue qui envoie du courrier indésirable en son nom en utilisant la liste des contacts de son client de messagerie. La probabilité que vous figuriez dans la liste des contacts de votre collègue est grande, ce qui signifie que votre boîte aux lettres sera certainement inondée de messages non sollicités. Dans ce cas, il est impossible de savoir, sur l'unique base de l'adresse de l'expéditeur, si le message a été envoyé par votre collègue ou par le spammeur. Utilisez l'en-tête du message ! Regardez attentivement qui a envoyé ce message, quand et quelle est sa taille. Suivez le parcours du message depuis l'expéditeur jusqu'à votre boîte aux lettres sur le serveur. Toutes ces informations doivent être reprises dans l'en-tête du message. Décidez si vous voulez télécharger ce message depuis le serveur ou le supprimer.

Remarque.

Vous pouvez trier les messages selon le titre de n'importe quelle colonne de la liste des messages. Pour trier les messages, cliquez sur le titre de la colonne. Le classement se fera dans l'ordre croissant. Pour modifier l'ordre du classement, cliquez à nouveau sur le titre de la colonne.

13.3.8. Actions à réaliser sur le courrier indésirable

Si l'analyse indique que le message est un exemplaire de courrier indésirable ou de courrier indésirable potentiel, la suite des opérations réalisées par Anti-Spam dépendra de l'état de l'objet et de l'action sélectionnée. Par défaut, les messages électroniques classés comme *courrier indésirable* ou *courrier indésirable potentiel* sont modifiés : Le texte **[!! SPAM]** ou **[?? Probable Spam]** est ajouté respectivement à l'**objet** du message.

Vous pouvez sélectionner des actions complémentaires à exécuter sur le courrier indésirable et le courrier indésirable potentiel. Des plug-ins spéciaux ont été prévus pour Microsoft Outlook et Microsoft Outlook Express et The Bat!. Pour les autres clients de messagerie, vous pouvez configurer les règles de tri.

13.3.9. Configuration du traitement du courrier indésirable dans Microsoft Office Outlook

N'oubliez pas que le plug in de recherche du courrier indésirable pour Microsoft Office Outlook est absent de l'application installée sous Microsoft Windows 9x.

Par défaut, le courrier qui est considéré comme *courrier indésirable* ou *courrier indésirable potentiel* est marqué à l'aide du texte **[!! SPAM]** ou **[?? Probable Spam]** dans l'**Objet**.

Les actions complémentaires à réaliser sur le courrier indésirable et le courrier indésirable potentiel dans Microsoft Office Outlook sont reprises sur l'onglet **Anti-Spam** du menu **Service → Paramètres** (cf. ill. 58).

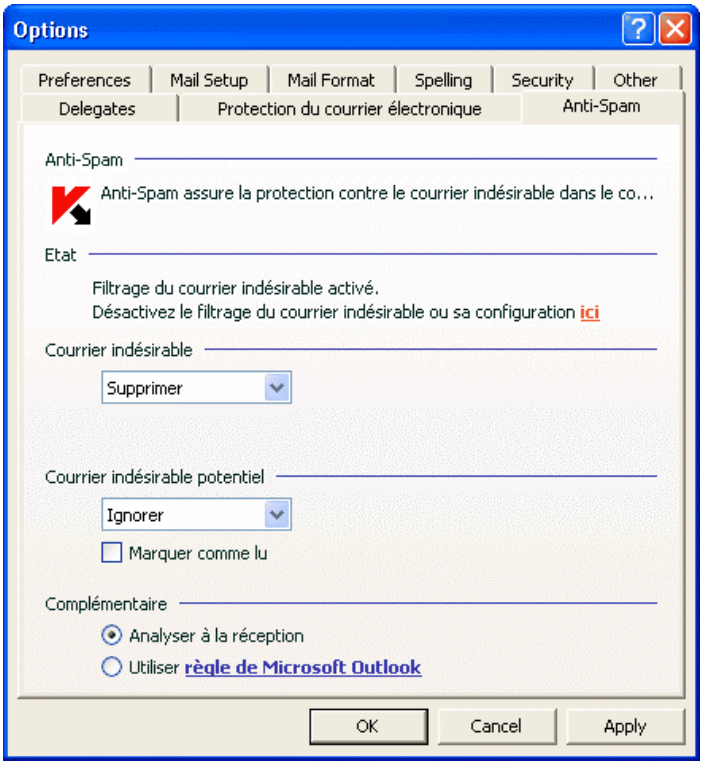


Illustration 58. Configuration détaillée du traitement du courrier indésirable dans Microsoft Office Outlook

Cet onglet s'ouvre automatiquement lors du premier chargement du client de messagerie après l'installation du programme et vous permet de configurer le traitement du courrier indésirable.

Les règles de traitement suivantes sont prévues aussi bien pour le courrier indésirable que pour le courrier indésirable potentiel :

Placer dans le dossier : le courrier indésirable est placé dans le dossier de la boîte aux lettres que vous aurez spécifié.

Copier dans le dossier : une copie du message est créée et placée dans le dossier indiqué. La copie originale reste dans le dossier **Entrant.**

Supprimer : supprime le courrier indésirable de la boîte aux lettres de l'utilisateur.

Ignorer : laisse le message électronique dans le dossier **Entrant**

Pour ce faire, sélectionnez la valeur souhaitée dans la liste déroulante du bloc **Courrier indésirable** ou **Courrier indésirable potentiel.**

Vous pouvez également indiquer l'algorithme de coopération entre Microsoft Office Outlook et Anti-Spam :

- **Analyser à la réception**. Tous les messages qui arrivent dans la boîte aux lettres de l'utilisateur sont d'abord analysés selon les règles définies de Microsoft Office Outlook. A la fin de ce traitement, les messages qui ne tombaient pas sous le coup de ces règles sont transmis au plug-in Anti-Spam. Le traitement se déroule dans un certain ordre. Cet ordre peut parfois ne pas être respecté, par exemple lors de la réception simultanée d'un grand nombre de messages dans la boîte aux lettres. Une telle situation peut faire que les informations relatives aux messages traités par les règles de Microsoft Office Outlook apparaissent comme *courrier indésirable* dans le rapport d'Anti-Spam. Afin d'éviter une telle situation, nous vous conseillons de configurer le plug-in d'Anti-Spam en qualité de règle de Microsoft Office Outlook .
- **Utiliser la règle de Microsoft Outlook**. Dans ce cas, le traitement des messages qui arrivent dans la boîte aux lettres de l'utilisateur s'opère selon la hiérarchie des règles de Microsoft Office Outlook. Il faut créer en guise de règle le traitement des messages par Anti-Spam. Il s'agit de l'algorithme de travail optimal qui évite les conflits entre Microsoft Outlook et le plug-in d'Anti-Spam. Cet algorithme a un seul défaut : la création et la suppression des règles de traitement des messages via Microsoft Office Outlook s'opère manuellement.

L'utilisation du plug-in d'Anti-Spam en qualité de règle de Microsoft Office Outlook n'est pas pris en charge dans Microsoft Office XP installé sous Microsoft Windows 9x/ME/NT en raison d'une erreur dans Microsoft Office Outlook XP.

Pour créer la règle de traitement d'un message à la recherche de courrier indésirable ::

1. Lancez Microsoft Office Outlook et utilisez la commande **Service→Règles et notifications** de la fenêtre principale du logiciel. La commande de lancement de l'Assistant dépend de la version de Microsoft Outlook que vous utilisez. Dans ce manuel, nous envisageons la création d'une règle dans Microsoft Office Outlook 2003.
2. Dans la fenêtre **Règles et notification** , passez à l'onglet **Règles pour le courrier électronique** et cliquez sur **Nouvelle**. Cette action entraîne le lancement de l'Assistant de création de nouvelle règle. Il contient les étapes suivantes :

   1ère étape

Vous devez choisir entre la création d'une règle "de zéro" ou au départ d'un modèle. Sélectionnez **Créer nouvelle règle** et en guise de condition de l'analyse, sélectionnez **Analyse des messages après la réception**. Cliquez sur **Suivant**.

2ème étape

Dans la fenêtre de sélection de la condition de rejet du message, cliquez sur **Suivant** sans avoir coché de cases. Confirmez l'application de cette règle à tous les messages reçus dans la fenêtre de confirmation.

3ème étape

Dans la fenêtre de sélection de l'action à réaliser sur les messages, cochez la case **Exécuter action complémentaire**. Dans la partie inférieure de la fenêtre, cliquez action complémentaire. Opérez votre sélection dans la liste déroulante **Kaspersky Anti-Spam** et cliquez sur **OK**.

4ème étape

Dans la fenêtre de sélection d'exclusion de la règle, cliquez sur **Suivant** sans avoir coché de cases

5ème étape

Dans la fenêtre de fin de la création de la règle, vous pouvez lui attribuer un nom (par défaut, il s'agira de **Kaspersky Anti-Spam**). Assurez-vous que la case **Activer la règle** est cochée puis, cliquez sur **Terminer**.

3. Par défaut, la nouvelle règle sera ajoutée en tête de la liste des règles de la fenêtre **Règles et notifications**. Déplacez cette règle à la fin de la liste si vous voulez qu'elle soit appliquée en dernier lieu au message.

Tous les messages qui arrivent dans la boîte aux lettres sont traités sur la base des règles. L'ordre d'application des règles dépend de la priorité associée à chaque règle. Les règles sont appliquées dans l'ordre de la liste. Chaque règle à une priorité inférieure à la règle précédente. Vous pouvez augmenter ou réduire la priorité d'application des règles au message.

Si vous souhaitez que le message, après l'exécution d'une règle quelconque, soit traité par une règle d'Anti-Spam, il faudra cocher la case **arrêter le traitement ultérieur des règles** dans les paramètres de cette règle (cf. 3ème étape de la fenêtre de création des règles).

Si vous avez de l'expérience dans la création de règles de traitement des messages dans Microsoft Office Outlook, vous pouvez créer une règle propre à Anti-Spam sur la base de l'algorithme proposé ci-dessus.

13.3.10. Configuration du traitement du courrier indésirable dans Microsoft Outlook Express

Par défaut, le courrier qui est considéré comme *courrier indésirable* ou *courrier indésirable potentiel* est marqué à l'aide du texte **[!! SPAM]** ou **[?? Probable Spam]** dans l'**Objet**.

Les actions complémentaires exécutées sur le courrier indésirable et le courrier indésirable potentiel dans Microsoft Outlook Express sont reprises dans une fenêtre spéciale (cf. ill. 59) qui s'ouvre après avoir cliqué sur le bouton **Configuration** situé à côté des autres boutons d'Anti-Spam dans la barre des tâches : **Courrier indésirable** et **Courrier normal**.

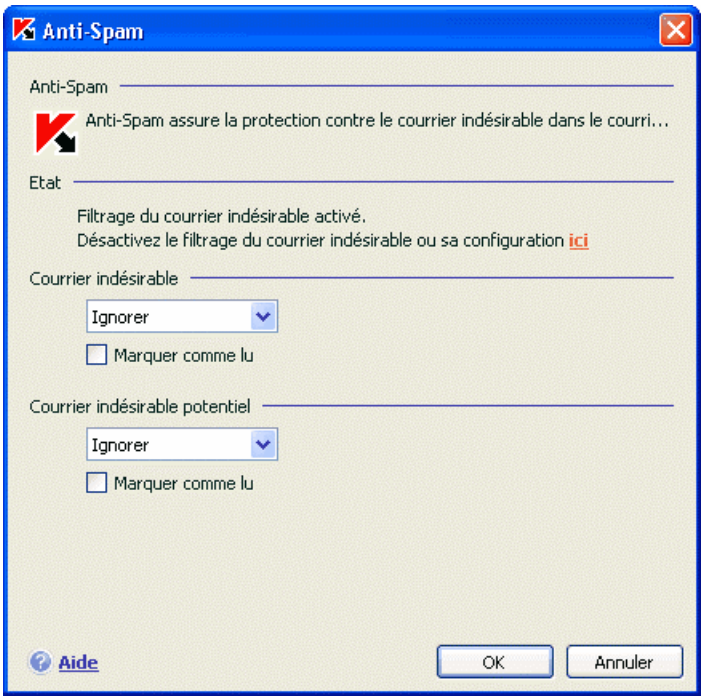


Illustration 59. Configuration détaillée du traitement du courrier indésirable dans Microsoft Outlook Express

La fenêtre s'ouvre automatiquement lors du premier chargement du client de messagerie après l'installation du programme et vous permet de configurer le traitement du courrier indésirable.

Les règles de traitement suivantes sont prévues aussi bien pour le courrier indésirable que pour le courrier indésirable potentiel :

Placer dans le dossier : le courrier indésirable est placé dans le dossier de la boîte aux lettres que vous aurez spécifié.

Copier dans le dossier : une copie du message est créée et placée dans le dossier indiqué. La copie originale reste dans le dossier **Entrant**.

Supprimer : supprime le courrier indésirable de la boîte aux lettres de l'utilisateur.

Ignorer : laisse le message électronique dans le dossier **Entrant**.

Pour ce faire, sélectionnez la valeur souhaitée dans la liste déroulante du bloc **Courrier indésirable** ou **Courrier indésirable potentiel**.

13.3.11. Configuration du traitement du courrier indésirable dans The Bat!

Les actions à exécuter sur le courrier indésirable et le courrier indésirable potentiel dans The Bat! sont définies à l'aides des outils du client.

Pour passer à la configuration des règles de traitement du courrier indésirable dans The Bat! :

1. Sélectionnez l'élément Configuration dans le menu Propriétés du client de messagerie.
2. Sélectionnez le nœud **Protection contre le courrier indésirable** (cf. ill. 60) dans l'arborescence des paramètres.

Les paramètres de protection contre le courrier indésirable sont appliqués à tous les modules antispam de l'ordinateur compatibles avec The Bat!

Vous devez définir le niveau d'évaluation et indiquer comment agir sur les messages correspondant au niveau défini (pour Anti-Spam, la probabilité que le message est un exemple de courrier indésirable) :

- Supprimer les messages dont le niveau d'évaluation est supérieur au niveau indiqué.
- Déplacer les messages du niveau défini dans un dossier spécial pour les messages non sollicités.
- Déplacer les messages non sollicités marqués d'une en-tête spéciale dans le dossier du courrier indésirable.

- Laisser les messages non sollicités dans le dossier **Entrant**.

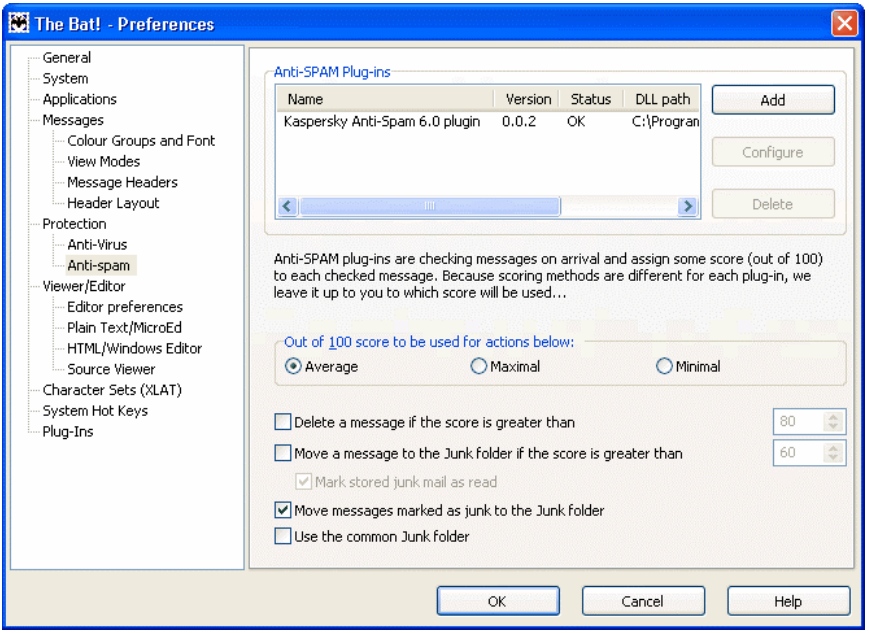


Illustration 60. Configuration de l'identification et du traitement du courrier indésirable dans The Bat!

Attention !

Suite au traitement des messages électroniques, Kaspersky Internet Security attribue le statut courrier indésirable ou courrier indésirable potentiel en fonction de facteurs (cf. point 13.3.3, p. 188) dont vous pouvez modifier la valeur. Dans The Bat!, on retrouve un algorithme spécial d'évaluation des messages qui repose également sur les facteurs de courrier indésirable. Afin d'éviter les écarts entre le facteur de courrier indésirable dans Kaspersky Internet Security et dans The Bat!, tous les messages analysés par Anti-Spam reçoivent une évaluation correspondant à l'état du message : *courrier normal :* 0%, *courrier indésirable potentiel* : *50 %*, courrier indésirable : *100 %*.

Ainsi, l'évaluation du message dans The Bat! correspond non pas au facteur du message attribué par Anti-Spam mais bien au facteur correspondant à l'état.

Pour de plus amples informations sur l'évaluation du courrier indésirable et sur les règles de traitement, consultez la documentation relative au client de messagerie The Bat!

CHAPITRE 14. RECHERCHE DE VIRUS SUR VOTRE ORDINATEUR

L'un des principaux composants de la protection antivirus de l'ordinateur est la recherche de virus dans les secteurs indiqués par l'utilisateur. Kaspersky Internet Security 2006 recherche la présence éventuelle de virus aussi bien dans des objets particuliers (fichiers, répertoires, disques, disques amovibles) que dans tout l'ordinateur. La recherche de virus exclut le risque de propagation d'un code malveillant qui n'aurait pas été repéré pour une raison quelconque par les autres composants de la protection.

Kaspersky Internet Security 2006 propose par défaut trois tâches de recherche de virus :

Secteurs critiques

Recherche de la présence éventuelle de virus dans tous les secteurs critiques de l'ordinateur. Il s'agit de : la mémoire système, des objets exécutés au démarrage du système, des secteurs d'amorçage des disques et des répertoires système *Windows* et *system32*. Cette tâche consiste à identifier rapidement dans le système tous les virus actifs sans lancer une analyse complète de l'ordinateur.

Mon poste de travail

Recherche de la présence éventuelle de virus sur votre ordinateur avec analyse minutieuse de tous les disques connectés, de la mémoire et des fichiers.

Objets de démarrage

Recherche de la présence éventuelle de virus dans les objets chargés lors du démarrage du système d'exploitation.

Par défaut, ces tâches sont exécutées selon les paramètres recommandés. Vous pouvez modifier ces paramètres (cf. point 14.4, p. 209) et même programmer le lancement de la tâche (cf. point 6.5, p. 85).

Il est possible également de créer des tâches personnalisées (cf. point 14.3, p. 208) de recherche de virus et de programmer leur lancement. Par exemple, il est possible de créer une tâche pour l'analyse des bases de messagerie une fois par semaine ou une tâche pour la recherche de la présence éventuelle de virus dans le répertoire **Mes documents**.

De plus, vous pouvez rechercher la présence éventuelle de virus dans n'importe quel objet (exemple : un des disques durs sur lequel se trouve les programmes et les jeux, les bases de messagerie ramenées du travail, les archives reçues par courrier électronique, etc.) sans devoir créer une tâche particulière. Vous pouvez sélectionner des objets individuels à analyser au départ de l'interface de Kaspersky Internet Security ou à l'aide des méthodes Microsoft Windows traditionnelles (ex. : dans la fenêtre de l'**Assistant** ou au départ du **Bureau**, etc.).

La section **Recherche de virus** dans la partie gauche de la fenêtre principale de l'application reprend la liste complète des tâches liées à la recherche de virus créées sur votre ordinateur.

14.1. Administration des tâches liées à la recherche de virus

Les tâches liées à la recherche de virus peuvent être lancées manuellement ou automatiquement selon un horaire défini (cf. point 6.5, p. 85).

Afin de lancer la tâche manuellement :

Sélectionnez le nom de la tâche dans la section **Analyser** de la fenêtre principale du logiciel et cliquez sur ▶ dans la barre d'état.

Pour suspendre l'exécution de la tâche :

Cliquez sur ❚❚ dans la barre d'état. L'état de l'exécution de la tâche devient *pause*. L'analyse sera suspendue jusqu'à ce que la tâche soit à nouveau relancée manuellement ou selon l'horaire.

Pour suspendre l'exécution de la tâche :

Cliquez sur ■ dans la barre d'état. L'état de l'exécution de la tâche devient *interrompue*. L'analyse sera arrêtée jusqu'à ce que la tâche soit à nouveau relancée manuellement ou selon l'horaire. Au moment du prochain lancement de la tâche vous pourrez soit reprendre la recherche là où elle a été interrompue ou en lancer une nouvelle.

14.2. Composition de la liste des objets à analyser

Afin de consulter la liste des objets qui seront analysés lors de l'exécution de la tâche, sélectionnez le nom de la tâche (ex. : **Mon poste de travail**) dans la

section **Analyser** dans la fenêtre principale du programme. La liste des objets sera reprise dans la partie droite de la fenêtre sous la barre d'état (cf. ill. 61).

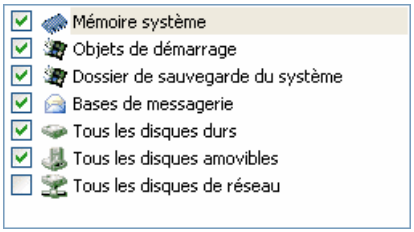


Illustration 61. Liste des objets à analyser

La liste des objets à analyser pour la liste des tâches créées par défaut lors de l'installation du logiciel est déjà composée. Lors de la création d'une tâche personnalisée ou lors de la sélection d'un objet dans le cadre de la recherche de virus, vous constituez vous-même la liste des objets.

Les boutons situés à droite de la liste vous permettront d'ajouter de nouveaux éléments ou de modifier la liste des objets à analyser. Afin d'ajouter un nouvel objet à analyser, cliquez sur **Ajouter** et indiquez l'objet dans la fenêtre qui s'affiche. Afin de supprimer un objet, sélectionnez-le dans la liste (son nom apparaîtra sur un fond gris) puis cliquez sur **Supprimer**. Vous pouvez suspendre temporairement l'analyse de certains objets sans avoir à les supprimer de la liste. Pour ce faire, il suffit de désélectionner la case qui se trouve en regard de l'objet qui ne doit pas être analysé.

Afin de lancer l'analyse, cliquez sur **Analyser** ou sélectionnez **Analyser!** dans le menu qui apparaît après avoir cliqué sur **Actions**.

De plus, vous pouvez sélectionner l'objet à analyser via les outils standard du système d'exploitation Microsoft Windows (exemple : via l'**Assistant** ou sur le **Bureau**, etc. (cf. ill. 62). Pour ce faire, placez la souris sur l'objet, ouvrez le menu contextuel d'un clic droit et sélectionnez **Rechercher d'éventuels virus**.

Illustration 62. Analyse d'un objet au départ du menu contextuel de Microsoft Windows

14.3. Création de tâches liées à la recherche de virus

Afin de rechercher la présence éventuelle de virus parmi les objets de votre ordinateur, vous pouvez soit utiliser les tâches d'analyse intégrées livrées avec le logiciel, soit utiliser des tâches personnalisées. La création d'une nouvelle tâche s'opère sur la base des tâches d'analyse existantes.

Afin de créer une nouvelle tâche d'analyse :

1. Dans la section **Analyser** de la fenêtre principale du logiciel, sélectionnez la tâche dont les paramètres vous conviennent le mieux.
2. Ouvrez le menu contextuel d'un clic droit de la souris ou cliquez sur le bouton **Actions** situés à droite de la liste des objets à analyser puis sélectionnez **Enregistrer sous**.
3. Saisissez, dans la fenêtre qui s'ouvre, le nom de la nouvelle tâche puis cliquez sur **OK**. La nouvelle tâche apparaît désormais sous le nom choisi dans la liste de tâches de la section **Analyser** de la fenêtre principale du logiciel.

Attention !

Le nombre de tâches que peut créer l'utilisateur est limité. Le nombre maximal est de quatre tâches.

La nouvelle tâche possède des paramètres identiques à ceux de la tâche qui lui a servi de fondation. Pour cette raison, vous devrez procéder à une configuration complémentaire : composer la liste des objets à analyser (cf. point 14.2, p. 206),

indiquer les paramètres d'exécution de la tâche (cf. point 14.4, p. 209) et, le cas échéant, programmer (cf. point 6.5, p. 85)le lancement automatique.

Afin de renommer une tâche :

sélectionnez la tâche dans la section **Analyser** de la fenêtre principale du logiciel, ouvrez le menu contextuel d'un clic droit de la souris ou cliquez sur le bouton **Actions** situé à droite de la liste des objets à analyser puis sélectionnez le point **Renommer**.

Saisissez, dans la fenêtre qui s'ouvre, le nouveau nom de la nouvelle tâche puis cliquez sur **OK**. Le nom de la tâche dans la section **Analyser** sera modifié.

Pour supprimer une tâche :

sélectionnez la tâche dans la section **Analyser** de la fenêtre principale du logiciel, ouvrez le menu contextuel d'un clic droit de la souris ou cliquez sur le bouton **Actions** situé à droite de la liste des objets à analyser puis sélectionnez le point **Supprimer**.

Confirmez la suppression de la tâche dans la boîte de dialogue de confirmation. La tâche sera ainsi supprimée de la liste des tâches dans la section **Analyser**.

Attention !

Vous pouvez uniquement renommer les tâches que vous avez créées.

14.4. Configuration des tâches liées à la recherche de virus

L'ensemble de paramètres définis pour chaque tâche détermine le mode d'exécution de l'analyse des objets sur l'ordinateur.

Afin de passer à la configuration des paramètres des tâches :

sélectionnez le nom de la tâche dans la section **Analyser** de la fenêtre principale et grâce au lien Configuration, ouvrez la boîte de dialogue de configuration des paramètres de la tâche.

La boîte de dialogue de configuration des tâches vous offre la possibilité de :

- sélectionner le niveau de protection pour l'exécution de la tâche (cf. point 14.4.1, p. 210);

- passer à la configuration détaillée du niveau :
    - indiquer les paramètres qui définissent les types de fichiers soumis à l'analyse antivirus (cf. point 14.4.2, p. 211);
    - configurer le lancement des tâches au nom d'un autre compte utilisateur (cf. point 6.4, p. 84);
    - définir les paramètres complémentaires de l'analyse (cf. point 14.4.5, p. 217);
- restaurer les paramètres d'analyse utilisés par défaut (cf. point 14.4.3, p. 214);
- sélectionner l'action qui sera exécutée en cas de découverte d'un objet infecté ou potentiellement infecté (cf. point 14.4.4, p. 214);
- programmer le lancement automatique de la tâche (cf. point 6.5, p. 85).

De plus, vous pouvez définir des paramètres uniques de lancement pour toutes les tâches (cf. point 14.4.6, p. 218).

Tous ces paramètres de configuration de la tâche sont abordés en détails ci-après.

14.4.1. Sélection du niveau de protection

Chaque tâche liée à la recherche de virus analyse les objets selon un des trois niveaux suivants (cf. ill. 63):

Elevé pour l'analyse complète en profondeur de votre ordinateur ou d'un disque, d'un répertoire ou d'un dossier particulier. Ce niveau est recommandé lorsque vous pensez que votre ordinateur a été infecté par un virus.

Recommandé. les paramètres de ce niveau correspondent aux paramètres recommandés par les experts de Kaspersky Lab. L'analyse porte sur les mêmes objets qu'au niveau **Elevé**, à l'exception des fichiers au format de courrier électronique.

Faible : ce niveau vous permet de travailler sans problèmes avec les applications gourmandes en mémoire vive car le volume de fichiers analysés est réduit.

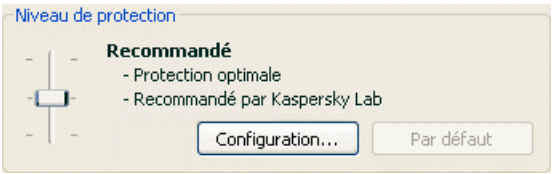


Illustration 63. Sélection du niveau de protection pour la recherche de virus

Par défaut, la protection des fichiers s'opère selon les paramètres du niveau **Recommandé**.

Vous pouvez augmenter ou réduire le niveau d'analyse des objets en sélectionnant un autre niveau ou en modifiant les paramètres du niveau actuel.

Pour modifier le niveau de protection :

Déplacez simplement le curseur. Ce faisant, vous modifiez le rapport entre la vitesse de l'analyse et la quantité d'objets analysés : plus le nombre de fichiers soumis à l'analyse sera réduit, plus la vitesse de l'analyse sera élevée

Si aucun des niveaux prédéfinis ne répond à vos attentes, vous pouvez procéder à une configuration complémentaire des paramètres de la protection. Dans ce cas, il est conseillé de choisir le niveau le plus proche de vos besoins en guise de point de départ et d'en modifier les paramètres. Dans ce cas, le niveau devient **Utilisateur**.

Pour modifier les paramètres du niveau de protection actuel :

cliquez sur **Configuration** dans la fenêtre de configuration de la tâche, modifiez les paramètres selon vos besoins et cliquez sur **OK**.

Un quatrième niveau de protection est ainsi configuré : **Utilisateur** selon les paramètres que vous aurez défini.

14.4.2. Définition du type d'objet analysé

La définition du type d'objet à analyser précise le format, la taille et l'emplacement des fichiers sur lesquels porte la tâche.

Le type de fichiers à analyser est défini dans la section **Types de fichiers** (cf. ill. 64). Choisissez l'une des trois options :

- **Analyser tous les fichiers**. Tous les objets sans exception seront analysés.
- **Analyser les programmes et les documents (selon le contenu).** Le programme analysera uniquement les fichiers qui présentent un risque d'infection, c.-à-d. les fichiers dans lesquels un virus pourrait s'insérer.

> Informations.
>
> Il existe des fichiers dans lesquels aucun virus ne peut s'incruster car le code du fichier ne contient aucun point d'accrochage pour le virus. Les fichiers texte en sont un exemple.

Avant de passer à la recherche de virus dans l'objet, le système définit le format du fichier (txt, doc, exe, etc.) en analysant l'en-tête interne du fichier.

Analyser les programmes et les documents (selon l'extension). Dans ce cas, le programme analyse uniquement les fichiers potentiellement infectés et le format du fichier est pris en compte sur la base de son extension. En cliquant sur l'extension, vous pourrez découvrir a liste des extensions des fichiers qui seront soumis à l'analyse dans ce cas (cf. point A.1, p. 290).

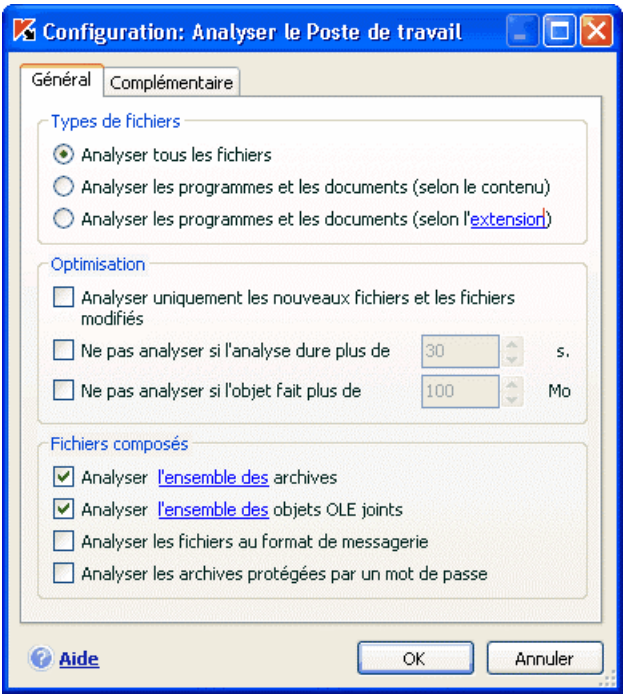


Illustration 64. Configuration des paramètres de l'analyse

Conseil.

Il ne faut pas oublier qu'une personne mal intentionnée peut envoyer un virus sur votre ordinateur dans un fichier dont l'extension est txt alors qu'il s'agit en fait d'un fichier exécutable renommer en fichier txt. Si vous sélectionnez l'option **Analyser les programmes et les documents (selon l'extension)**, ce fichier sera ignoré pendant l'analyse. Si vous sélectionnez l'option **Analyser les programmes et les documents (selon le contenu)**, le programme ignorera l'extension, analysera l'en-tête du fichier et découvrira qu'il s'agit d'un fichier exe. Le fichier sera alors soumis à une analyse antivirus minutieuse.

Vous pouvez, dans la section **Optimisation**, préciser que seuls les nouveaux fichiers et ceux qui ont été modifiés depuis la dernière analyse, seront soumis à

l'analyse antivirus. Ce mode réduit considérablement la durée de l'analyse et augmente la vitesse de traitement du logiciel. Pour ce faire, il est indispensable de cocher la case ☑ **Analyser uniquement les nouveaux fichiers et les fichiers modifiés**. Ce mode de travail touchera aussi bien les fichiers simples que les fichiers composés.

Vous pouvez aussi, dans la section **Optimisation**, instaurer une limite sur la durée de l'analyse et la taille maximale d'un objet:

- ☑ **Ne pas analyser si l'analyse dure plus de…s**. Cochez cette case afin de limiter dans le temps l'analyse d'un objet et saisissez dans le champ de droite la durée maximale autorisée pour l'analyse. Si cette valeur est dépassée, l'objet sera exclu de l'analyse.
- ☑ **Ne pas analyser si l'objet fait plus de … Mo**. Cochez cette case pour limiter au niveau de la taille l'analyse des objets et saisissez dans le champ de droite la taille maximale autorisée. Si cette valeur est dépassée, l'objet est exclu de l'analyse.

Indiquez, dans la section **Fichiers composés**, les types de fichiers composés qui devront être soumis à l'analyse antivirus :

- ☑ **Analyser l'ensemble des/uniquement les nouveaux(-elles) archives** : analyse les archives au format ZIP, CAB, RAR, ARJ, LHA, JAR, ICE
- ☑ **Analyser l'ensemble des/uniquement les nouveaux(-elles) objets OLE joints** : analyse les objets intégrés au fichier (ex. : tableau Excel ou macro dans Word, pièce jointe d'un message, etc.)

Pour chaque type de fichier composé, vous pouvez décider d'analyser tous les fichiers ou uniquement les nouveaux. Pour ce faire, cliquez sur le lien situé en regard du nom de l'objet. Il change de valeur lorsque vous appuyez sur le bouton gauche de la souris. Si vous avez défini dans la section **Optimisation** l'analyse uniquement des nouveaux fichiers et des fichiers modifiés, il sera impossible de sélectionner un type de fichier composé.

- ☑ **Analyser les fichiers au format de messagerie** : analyse les fichiers au format de courrier électronique ainsi que les bases de données de messagerie. Si la case n'a pas été cochée, les fichiers au format de messagerie ne seront pas analysés et le statut *ok* sera attribué à l'objet dans le rapport.

Nous attirons votre attention sur les particularités suivantes de l'analyse de bases de messagerie protégées par un mot de passe :

- Kaspersky Internet Security identifie le code malveillant dans les bases de messagerie de Microsoft Office Outlook 2000 mais ne les répare pas;
- Le programme ne prend pas en charge la recherche de code malveillant dans les bases de messagerie de Microsoft Office Outlook 2003 protégées par un mot de passe.

☑ **Analyser les archives protégées par un mot de passe** : active l'analyse des archives protégées par un mot de passe. La boîte de dialogue de saisie du mot de passe s'affichera avant de procéder à l'analyse des objets de l'archive. Si la case n'est pas cochée, les archives protégées par un mot de passe seront ignorées.

14.4.3. Restauration des paramètres d'analyse par défaut

Lorsque vous configurez les paramètres d'exécution d'une tâche, vous avez toujours la possibilité de revenir aux paramètres recommandés. Il s'agit des paramètres optimum recommandés par les experts de Kaspersky Lab et regroupés au sein du niveau de protection **Recommandé**.

Pour restaurer les paramètres de protection des fichiers par défaut :

1. Sélectionnez le nom de la tâche dans la section **Recherche de virus** de la fenêtre principale et grâce au lien Configuration, ouvrez la boîte de dialogue de configuration des paramètres de la tâche.
2. Cliquez sur le bouton **Par défaut** dans le bloc **Niveau de protection.**

14.4.4. Sélection de l'action exécutée sur les objets

Si l'analyse d'un objet détermine une infection ou une possibilité d'infection, la suite du fonctionnement du programme dépendra de l'état de l'objet et de l'action sélectionnée.

A la fin de l'analyse, chaque objet peut se voir attribuer l'un des statuts suivants :

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

- *Potentiellement infecté* lorsqu'il n'est pas possible d'affirmer avec certitude si l'objet est infecté ou non. Cela signifie que le code du fichier contient une séquence semblable à celle d'un virus connu mais modifié ou qui évoque, par sa structure, la séquence d'un virus.

Par défaut, tous les objets infectés sont réparés et tous les objets suspects sont placés en quarantaine.

Pour modifier l'action à exécuter sur l'objet :

sélectionnez le nom de la tâche dans la section **Recherche de virus** de la fenêtre principale et grâce au lien Configuration, ouvrez la boîte de dialogue de configuration de la tâche. Toutes les actions possibles sont reprises dans la section correspondante (cf. ill. 65).

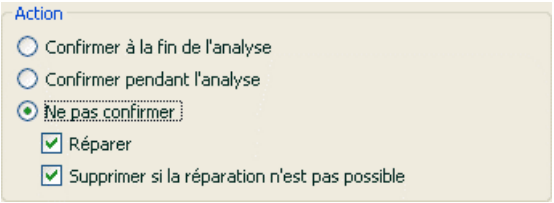


Illustration 65. Sélection de l'action à réaliser sur l'objet dangereux

Action choisie	**Conséquence en cas de découverte d'un objet malveillant/potentiellement infecté**
Confirmer à la fin de l'analyse	Le programme reporte le traitement des objets jusque la fin de l'analyse. Une fenêtre contenant les statistiques avec la liste des objets découverts apparaîtra à la fin de l'analyse et vous pourrez choisir le traitement à réaliser.
Confirmer pendant l'analyse	Le programme affiche un message d'avertissement qui reprend les informations relatives au code malveillant source de l'infection (potentielle) et propose l'une des actions suivantes.

Ne pas confirmer	Le programme consigne les informations relatives aux objets découverts dans le rapport sans les avoir traités ou sans avoir averti l'utilisateur. Ce mode n'est pas recommandé car il ne débarrasse pas votre ordinateur des objets infectés et potentiellement infectés, ce qui conduira inévitablement à l'infection de celui-ci.
Ne pas confirmer **Réparer**	Le programme, sans avertir au préalable l'utilisateur, tente de réparer l'objet découvert. Si la tentative échoue, l'objet est placé en quarantaine (cf. point 16.1, p. 231). Les informations relatives à cette situation sont consignées dans le rapport (cf. point 16.3, p. 237). Il est possible de tenter de réparer cet objet ultérieurement.
Ne pas confirmer **Réparer** **Supprimer si la réparation n'est pas possible**	Le programme, sans avertir au préalable l'utilisateur, tente de réparer l'objet découvert. Si la réparation de l'objet échoue, il sera supprimé.
Ne pas confirmer **Réparer** **Supprimer**	Le programme supprimera automatiquement l'objet.

Quel que soit le statut de l'objet (infecté ou potentiellement infecté), Kaspersky Internet Security crée une copie de sauvegarde avant de tenter de le réparer ou de le supprimer. Cette copie est placée dans le dossier de sauvegarde (cf. point 16.2, p. 235)au cas où il faudrait restaurer l'objet ou si la réparation devenait possible.

14.4.5. Paramètres complémentaires pour la recherche de virus

En plus de la configuration des paramètres principaux de la recherche de virus, vous pouvez également définir des paramètres complémentaires (cf. ill. 66):

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

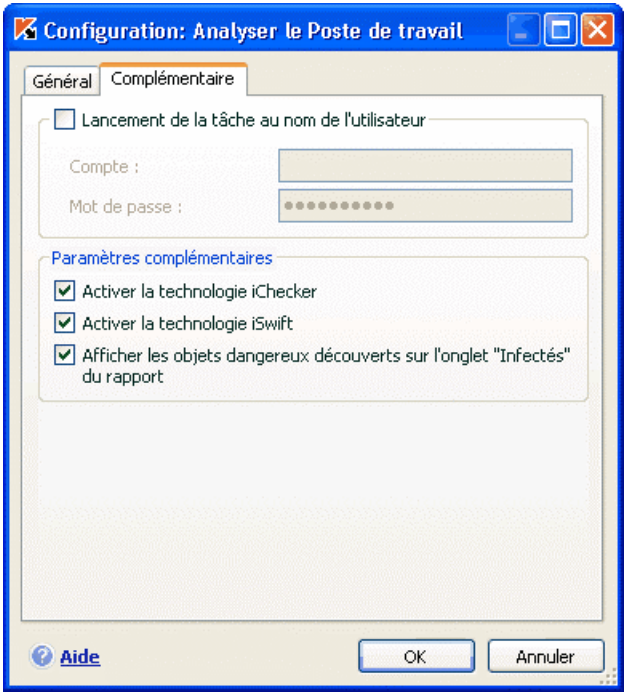


Illustration 66. Configuration complémentaire de l'analyse

Admettons que vous ayez une archive qui a été analysée par le programme et qui est saine. Lors de la prochaine analyse, cet objet sera exclu pour autant qu'aucune modification n'ait été apportée au fichier en question ou aux paramètres de l'analyse. Si vous avez changé le contenu

de l'archive (ex. : ajout d'un nouvel objet), si vous avez modifié les paramètres de l'analyse ou procédé à la mise à jour des bases des signatures des menaces, l'archive sera analysée à nouveau.
La technologie iChecker™ a ses limites : elle ne s'applique qu'aux objets dont la structure est connue de Kaspersky Internet Security (exemple : fichiers exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar).

Activer la technologie iSwift : utilise la technologie qui permet d'augmenter la vitesse de l'analyse en limitant celle-ci uniquement aux objets nouveaux ou modifiés. La technologie iSwift a ses limites : elle s'applique uniquement aux objets du système de fichiers NTFS.

> Le recours à la technologie iSwift n'est pas disponible sous Microsoft Windows XP64.

Afficher les objets dangereux sur l'onglet "Infectés" : affiche la liste des menaces découvertes sur l'onglet Infectés de la fenêtre du rapport (cf. point 16.3.2, p. 241). La désactivation de cette fonction peut être utile lors d'une analyse spéciale, par exemple en cas d'analyse de collections d'essai afin d'augmenter la vitesse d'analyse.

14.4.6. Définition de paramètres d'analyse uniques pour toutes les tâches

Chaque tâche d'analyse s'exécute en fonction de ses paramètres. Les tâches créées lors de l'installation du programme sur l'ordinateur sont exécutées par défaut selon les paramètres recommandés par les experts de Kaspersky Lab.

Vous pouvez configurer des paramètres d'analyse uniques pour toutes les tâches. La sélection de paramètres utilisée pour la recherche de virus dans un objet particulier servira de base.

Afin de définir des paramètres d'analyse uniques pour toutes les tâches :

1. Sélectionnez la section **Analyser** dans la partie gauche de l'onglet et cliquez sur le lien Configuration.
2. Dans la boîte de dialogue de configuration qui s'affiche, définissez les paramètres de l'analyse : sélectionnez le niveau de protection (cf. point 14.4.1, p. 210), réalisez la configuration complémentaire du niveau et indiquez l'action qui sera réalisée sur les objets (cf. point 14.4.4, p. 214).
3. Afin d'appliquer les paramètres définis à toutes les tâches, cliquez sur **Appuyer** dans la section **Paramètres des autres tâches**. Confirmez les paramètres uniques dans la boîte de dialogue de confirmation.

CHAPITRE 15. MISE A JOUR DU LOGICIEL

L'actualité de la protection est le garant de la sécurité de votre ordinateur. Chaque jour, de nouveaux virus, chevaux de Troie et autres programmes malveillant apparaissent. Il est donc primordial de s'assurer que vos données sont bien protégées.

La mise à jour du logiciel suppose le téléchargement et l'installation sur votre ordinateur des :

- Signature des menaces

  La protection de vos données est réalisée à l'aide des signatures des menaces. Elles sont utilisées par les composants de la protection pour rechercher les objets dangereux sur votre ordinateur et les neutraliser. Ces signatures sont enrichies toutes les heures des définitions des nouvelles menaces et des moyens de lutter contre celles-ci. Pour cette raison, il est vivement recommandé de les actualiser régulièrement.

  Les versions antérieures des logiciels antivirus de Kaspersky Lab prenaient en charge l'utilisation de différentes bases de signatures des menaces : standard ou étendues. Elles se différenciaient par le type d'objets dangereux contre lesquels elles assuraient une protection. Avec Kaspersky Internet Security, il n'est plus nécessaire de se soucier du choix des bases de signatures des menaces adéquates. Nos logiciels utilisent désormais les signatures des menaces qui offrent une protection non seulement contre divers types de programmes malveillants et d'objets présentant un risque potentiel, mais également contre les attaques de pirates informatiques.

- modules logiciels

  En plus des signatures des menaces connues, vous pouvez actualiser les modules logiciels de Kaspersky Internet Security. Ces mises à jour sont diffusées régulièrement par Kaspersky Lab.

Les serveurs spéciaux de mise à jour de Kaspersky Lab sont les principales sources pour obtenir les mises à jour de Kaspersky Internet Security. En voici quelques-uns :

http://downloads1.kaspersky-labs.com/updates/

http://downloads2.kaspersky-labs.com/updates/

ftp://downloads1.kaspersky-labs.com/updates/, etc.

Afin de pouvoir télécharger ces bases , votre ordinateur doit absolument être connecté à Internet.

Le téléchargement des mises à jour s'opère selon l'un des modes suivants :

- *Automatique*. Dans ce cas, Kaspersky Internet Security lance la copie et l'installation de mises à jour au fur et à mesure qu'elles sont publiées sur le serveur.
- *Programmé*. La mise à jour du logiciel est réalisée selon un horaire défini.
- *Manuel*. Vous lancez vous-même la procédure de mise à jour du logiciel.

Au cours du processus, les modules logiciels et les signatures des menaces installés sur votre ordinateur sont comparés à ceux du serveur. Si les signatures et les composants installés sur votre ordinateur sont toujours d'actualité, le message correspondant apparaîtra à l'écran. Si les signatures et les modules diffèrent, la partie manquante de la mise à jour sera installée. La copie des signatures et des modules complets n'a pas lieu, ce qui permet d'augmenter sensiblement la vitesse de la mise à jour et de réduire le volume du trafic.

Avant de lancer la mise à jour des signatures des menaces, Kaspersky Internet Security réalise une copie des signatures installées au cas où vous souhaiteriez à nouveau l'utiliser pour une raison quelconque.

La possibilité d'annuler (cf. point 15.2, p. 221) une mise à jour est indispensable, par exemple si les signatures des menaces que vous avez téléchargées sont corrompues. Vous pouvez ainsi revenir à la version précédente et tenter de les actualiser à nouveau ultérieurement.

.

15.1. Lancement de la mise à jour

Vous pouvez lancer la mise à jour du logiciel à n'importe quel moment. Celle-ci sera réalisée au départ de la source de la mise à jour que vous aurez choisie (cf. point 15.3.1, p. 222).

Vous pouvez lancer la mise à jour du logiciel depuis :

- le menu contextuel (cf. point 4.2, p. 48);
- la fenêtre principale du logiciel (cf. point 4.3, p. 49).

Pour lancer la mise à jour du logiciel depuis le menu contextuel :

1. Ouvrez le menu à l'aide d'un clic droit sur l'icône du logiciel dans la barre des tâches.
2. Sélectionnez le point **Mise à jour**.

Pour lancer la mise à jour du logiciel depuis la fenêtre principale du logiciel :

1. Sélectionnez le composant **Mise à jour** dans la section **Service**.
2. Cliquez sur le bouton **Mettre à jour** (appel du programme depuis l'aide) dans la partie droite de la fenêtre principale ou sur ▶ dans la barre d'état.

Le processus de mise à jour du logiciel sera illustré dans une fenêtre spéciale. Vous pouvez dissimuler la fenêtre avec les résultats actuels de la mise à jour. Pour ce faire, cliquez sur Fermer. La mise à jour ne sera pas interrompue.

15.2. Annulation de la dernière mise à jour

Chaque fois que vous lancez la mise à jour du logiciel, Kaspersky Internet Security commence par créer une copie de sauvegarde de la version actuelle des signatures des menaces avant de les actualiser. Cela vous donne la possibilité d'utiliser à nouveau la version antérieure des signatures après une mise à jour ratée.

Cette possibilité d'annuler la mise à jour est utile si, par exemple, une partie des signatures a été corrompue suite à une déconnexion pendant la mise à jour. Vous pouvez ainsi revenir à la version précédente et tenter d'actualiser à nouveau les signatures ultérieurement.

Pour revenir à l'utilisation de la version précédente des signatures des menaces:

1. Sélectionnez le composant **Mise à jour** dans la section **Service** dans la fenêtre principale du logiciel.
2. Cliquez sur le bouton **Retour à l'état précédent** (appel du programme depuis l'aide) dans la partie droite de la fenêtre principale).

15.3. Configuration de la mise à jour

La mise à jour du logiciel s'exécute selon les paramètres qui définissent :

- la ressource d'où les fichiers seront copiés avant d'être installés (cf. point 15.3.1, p. 222);
- le mode de lancement de la mise à jour du logiciel (cf. point 15.3.2, p. 225);
- les éléments actualisés

- les actions à réaliser après la mise à jour du logiciel (cf. point 15.3.4, p. 229).

Tous ces paramètres sont abordés en détails ci-après.

15.3.1. Sélection de la source de la mise à jour

La source de la mise à jour est une ressource quelconque qui contient les mises à jour des signatures des menaces et des modules logiciels de Kaspersky Internet Security. Il peut s'agir d'un serveur HTTP ou FTP, voire d'un répertoire local ou de réseau.

Les *serveurs de mise à jour de Kaspersky Lab* constituent la source principale de mise à jour. Il s'agit de sites Internet spéciaux prévus pour la diffusion des signatures des menaces et des modules logiciels pour tous les produits de Kaspersky Lab.

Attention !

Lors de la commande des mises à jour sur disque amovible, précisez si vous souhaitez recevoir la mise à jour des modules de l'application.

Les mises à jour obtenues sur un disque amovible peuvent être par la suite placées sur un site FTP ou HTPP ou dans un répertoire local ou de réseau.

La sélection de la source de la mise à jour s'opère dans l'onglet **Source de mise à jour** (cf. ill. 67).

Par défaut, la liste contient uniquement les serveurs de mise à jour de Kaspersky Lab. Cette liste n'est pas modifiable. Lors de la mise à jour, Kaspersky Internet Security consulte cette liste, contacte le premier serveur de la liste et tente de télécharger les mises à jour. Lorsque l'adresse sélectionnée ne répond pas, le logiciel choisit le serveur suivant et tente à nouveau de télécharger les bases antivirus. L'adresse du serveur au départ duquel la mise à jour sera téléchargée sera placée automatiquement au début de la liste. Lors de le mise à jour suivante depuis les serveurs de Kaspersky Lab, le logiciel contactera en premier lieu le serveur ayant fourni la mise à jour précédente.

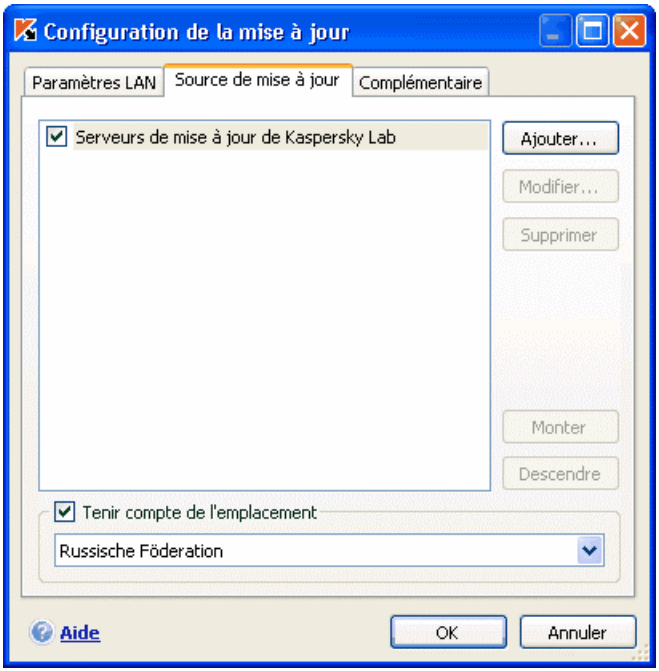


Illustration 67. Sélection de la source de la mise à jour

Pour réaliser la mise à jour au départ d'un site FTP ou HTTP quelconque :

1. Cliquez sur **Ajouter** ;
2. Sélectionnez le site FTP ou HTTP dans la fenêtre **Sélection de la source de mise à jour** ou indiquez son adresse IP, son nom symbolique ou l'URL dans le champ **Source**.

Attention !

Si vous avez sélectionné une ressource de réseau (serveurs de Kaspersky Lab ou un site FTP ou HTTP quelconque) en guise de source de mise à jour, il faudra prévoir un accès Internet.

Pour actualiser le logiciel au départ d'un répertoire quelconque :

1. Cliquez sur **Ajouter** ;
2. Sélectionnez le répertoire dans la fenêtre **Sélection de la source de la mise à jour** ou saisissez son chemin d'accès complet dans le champ **Source**.

Kaspersky Internet Security ajoute la nouvelle source de mise à jour au début de la liste et l'active automatiquement (la case en regard est cochée).

Si plusieurs ressources ont été sélectionnées en guise de source de mise à jour, le logiciel les consultera dans l'ordre de la liste et réalisera la mise à jour au départ de la première source disponible. Vous pouvez modifier l'ordre des sources dans la liste à l'aide des boutons **Monter**/**Descendre**

Modifiez la liste des sources à l'aide des boutons **Ajouter**, **Modifier**, **Supprimer**. Les serveurs de mise à jour de Kaspersky Lab sont les seules sources qui ne peuvent pas être modifiées ou supprimées.

Il existe un autre aspect qui peut être réglé lors de la mise à jour des signatures des menaces, à savoir le format de la mise à jour. Les signatures des menaces reprennent un fichier XML qui décrit la structure des répertoires contenant la mise à jour. Cette structure intervient dans la mise à jour des signatures sur l'ordinateur. La structure actuelle de la mise à jour des signatures des menaces est différente de la structure des bases utilisées dans les versions antérieures des applications de Kaspersky Lab.

Si vous réalisez la mise à jour non pas au départ des serveurs de mise à jour de Kaspersky Lab, mais au départ d'une archive zip ou d'un répertoire quelconque qui ne prend pas en charge la structure standard des répertoires des signatures des menaces, il est conseillé de cocher la case **Mise à jour depuis un dossier ou d'une archive zip non structuré (entraîne un ralentissement de la mise à jour)**. Ce paramètre ralentit quelque peu la mise à jour mais permet d'éviter les erreurs.

Si vous utilisez les serveurs de Kaspersky Lab en guise de serveur de mise à jour, vous pouvez sélectionner le serveur en fonction de la situation géographique qui vous convient le mieux. Kaspersky Lab possède des serveurs dans plusieurs pays. En choisissant le serveur situé le plus proche de vous géographiquement, vous pouvez augmenter la vitesse de la mise à jour et du téléchargement de celle-ci.

Afin de sélectionner le serveur le plus proche, cochez la case **Tenir compte de l'emplacement** et, dans la liste déroulante, sélectionnez le pays le plus proche de votre situation géographique actuelle.

N'oubliez pas que vous ne pourrez pas sélectionner le serveur le plus proche de votre situation géographique si le logiciel est installé sous Windows 9x/NT 4.0.

15.3.2. Sélection du mode et des objets de la mise à jour

La définition des objets à mettre à jour et du mode de mise à jour est l'un des moments décisifs de la configuration de la mise à jour.

Les objet de la mise à jour (cf. ill. 68) désignent les objets qui seront actualisés : les signatures des menaces, les modules de l'application ou la liste des attaques de réseau utilisée Anti-Hacker. Les signatures des menaces sont toujours actualisées tandis que la mise à jour modules de l'application ou des informations relatives aux attaques de réseau a lieu uniquement si l'option a été configurée.

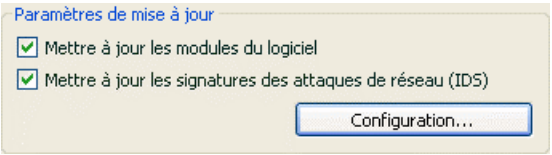


Illustration 68. Sélection des objets de la mise à jour

Pour copier et installer les mises à jour des modules de l'application pendant la mise à jour :

Cochez la case **Mettre à jour les modules de l'application** dans la fenêtre de configuration du composant Mise à jour.

Si une mise à jour des modules de l'application est présente à ce moment dans la source, le programme recevra les mises à jour requises et les appliquera après le redémarrage de l'ordinateur. Les mises à jour téléchargées ne seront pas installées tant que l'ordinateur ne sera pas redémarré.

Si la mise à jour suivante se produit avant le redémarrage de l'ordinateur, et l'installation des mises à jour antérieure des modules de l'application, seule la mise à jour des signatures des menaces aura lieu.

Afin que les informations relatives aux nouvelles attaques de réseau et aux moyens de les bloquer soient copiées et installées,

Cochez la case **Mettre à jour les pilotes de réseau et les signatures des attaques (IDS)** dans la fenêtre de configuration du composant Mise à jour

Le mode de mise à jour du logiciel (cf. ill. 69) désigne la manière dont la mise à jour sera lancée. Choisissez l'un des modes suivants :

Automatique. Dans ce cas, Kaspersky Internet Security lance la copie et l'installation des mises à jour au fur et à mesure qu'elles sont publiées sur le serveur ou sur d'autres sources (cf. point 15.3.1, p. 222). Ce mode de mise à jour est activé par défaut.

Si vous vous connectez à Internet à l'aide d'un modem et que vous avez choisi une ressource de réseau en tant que source de mise à jour, Kaspersky Internet Security tentera de réaliser la mise à jour chaque fois que la connexion sera établie ou selon un intervalle défini lors de la mise à jour antérieure. Les mises à jour réalisées au départ d'une source locales ont lieu à l'intervalle défini lors de la mise à jour précédente. Cela permet de régler automatiquement la fréquence des mises à jour en cas d'épidémie de virus ou d'autres situations dangereuses. Le logiciel recevra en temps opportuns les versions les plus récentes des signatures des menaces , des modules de l'application ou des attaques de réseau, ce qui réduira à zéro le risque d'infection de votre ordinateur par des programmes dangereux.

Illustration 69. Sélection du mode de lancement de la mise à jour

Tous les 1 jour(s). La mise à jour du logiciel est réalisée selon un horaire défini. Si vous souhaitez activer ce mode, la mise à jour sera réalisée par défaut chaque à jour. Pour composer un autre horaire, cliquez sur **Modifier** à côté du nom du mode et réalisez les modifications souhaitées dans la boîte de dialogue qui s'ouvre (pour de plus amples renseignements, consultez le point 6.5 à la page 85).

Manuel. Vous lancez vous-même la procédure de mise à jour du logiciel. Kaspersky Internet Security vous avertira de la nécessité de réaliser la mise à jour :

- Tout d'abord, une infobulle apparaît au-dessus de l'icône de l'application dans la barre des tâches (cf. point 16.10.1, p. 266);
- Ensuite, le deuxième indice dans la fenêtre principale de l'application vous signale que la protection de l'ordinateur est dépassée (cf. point 5.1.1, p. 55);
- Troisièmement, la section des commentaires et des conseils de la fenêtre principale affiche des conseils sur la mise à jour du logiciel (cf. point 4.3, p. 49).

15.3.3. Configuration des paramètres de connexion

Si vous avez sélectionné les serveurs de mise à jour de Kaspersky Lab ou un serveur FTP ou HTTP quelconque en tant que source de mise à jour, nous vous conseillons de vérifier les paramètres de connexion à Internet.

Par défaut, la connexion à Internet est réalisée selon les paramètres repris dans le navigateur (par exemple, Microsoft Internet Explorer). Ils devront peut-être être modifiés. Il est important de savoir si l'accès à Internet est réalisé via un serveur proxy et un pare-feu. Contactez votre administrateur système ou posez la question à votre fournisseur d'accès.

Tous les paramètres sont regroupés sur l'onglet spécial **Paramètres LAN** (cf. ill. 70).

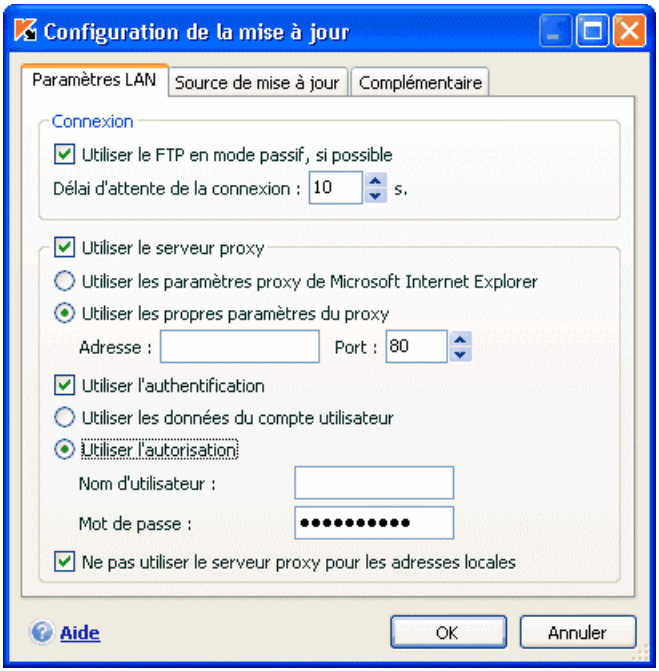


Illustration 70. Configuration des paramètres de réseau de la mise à jour

Le paramètre **Utiliser le FTP en mode passif, si possible** est utilisé lorsque vous téléchargez les mises à jour depuis un serveur FTP auquel vous vous

connectez en mode passif (par exemple, via un pare-feu). Si la connexion s'effectue en mode actif, vous pouvez désélectionnez cette case.

Si la connexion à Internet s'opère via un serveur proxy, cochez la cas ☑ **Utiliser le serveur proxy** et, le cas échéant, configurez les paramètres suivants :

- Sélectionnez les paramètres du serveur proxy à utiliser pour la mise à jour :

  ◉ **Utiliser les paramètres proxy de Microsoft Internet Explorer** : utilise le serveur proxy indiqué dans les paramètres de connexion de Microsoft Internet Explorer.

  ◉ **Utiliser les propres paramètres du proxy** : utilise un serveur proxy différent de celui indiqué dans les paramètres de connexion du navigateur. Saisissez l'adresse IP ou le nom symbolique dans le champ **Adresse** et dans le champ **Port**, le port du serveur proxy prévu pour la mise à jour du programme.

- Indiquez si l'authentification est requise sur le proxy. L'authentification est une procédure qui vérifie vos droits d'accès au serveur proxy en fonction de vos données d'enregistrement. Si l'authentification est requise pour la connexion à Internet, cochez la case ☑ **Utiliser l'authentification**.

- Sélectionnez le mode d'enregistrement sur le serveur proxy lors de l'accès à Internet :

  ◉ **Utiliser les données du compte utilisateur** : pour l'accès à Internet, les données du compte de l'utilisateur sur cet ordinateur et dans le domaine sont utilisées.

  > Remarque.
  >
  > Les données du compte utilisateur ne sont pas utilisées lorsque le logiciel fonctionne sur un ordinateur tournant sous Microsoft Windows 9X qui ne fait pas partie du domaine.

  ◉ **Utiliser l'autorisation**. Le processus d'autorisation vérifie votre nom et mot de passe. Saisissez les données correspondantes dans les champs **Nom d'utilisateur** et **Mot de passe**.

Afin de ne pas utiliser le serveur proxy lors de la mise à jour depuis un répertoire local ou de réseau, désélectionnez la case ☑ **Ne pas utiliser le serveur proxy pour les adresses locales**.

> Ce paramètre n'est pas disponible si le logiciel est installé sous Microsoft Windows 9X/NT 4.0. Toutefois, le serveur proxy pour les adresses locales n'est pas utilisé par défaut.

15.3.4. Actions exécutées après la mise à jour du logiciel

Chaque mise à jour des signatures des menaces contient de nouvelles définitions capables de protéger votre ordinateur contre les menaces récentes.

Les experts de Kaspersky Lab vous recommandent d'analyser *les objets en quarantaine et les objets de démarrage directement* après la mise à jour.

Pourquoi ces objets et pas d'autres ?

La quarantaine contient des objets dont l'analyse n'a pas pu définir avec certitude le type de programme malicieux qui les a infecté (cf. point 16.1, p. 231). Il se peut que la version actualisée des signatures des menaces de Kaspersky Internet Security puisse reconnaître et neutraliser le danger.

Par défaut, le logiciel analyse les objets en quarantaine après chaque mise à jour des signatures des menaces connues. Nous vous conseillons d'examiner fréquemment les objets en quarantaine. Leur statut peut changer après l'analyse. Certains objets pourront être restaurés dans leur emplacement d'origine et à nouveau utilisés.

Pour annuler l'analyse des objets en quarantaine, désélectionnez la case **Analyser les fichiers en quarantaine** dans le bloc **Action après la mise à jour**.

Les objets de démarrage représentent un secteur critique dans le domaine de la sécurité de votre ordinateur. Si ce secteur est infecté par un programme malicieux, il se peut que vous ne parveniez plus à lancer le système d'exploitation. Kaspersky Internet Security propose une tâche d'analyse des objets de démarrage (cf. Chapitre 14, p. 205). Il est conseillé de configurer le lancement automatique de cette tâche après chaque mise à jour des signatures des menaces (cf. point 6.5, p. 85).

CHAPITRE 16. POSSIBILITES COMPLEMENTAIRES

En plus de protéger vos données, le logiciel propose des services complémentaires qui élargissent les possibilités de Kaspersky Internet Security.

Au cours de ses activités, le logiciel place certains objets dans des répertoires spéciaux. L'objectif suivi est d'offrir une protection maximale avec un minimum de pertes.

- Le dossier de sauvegarde contient les copies des objets qui ont été modifiés ou supprimés par Kaspersky Internet Security (cf. point 16.2, p. 235). Si un objet qui contenait des informations importantes n'a pu être complètement préservé pendant le traitement antivirus, vous pourrez toujours le restaurer au départ de la copie de sauvegarde.
- La quarantaine contient les objets potentiellement infectés qui n'ont pas pu être traités avec les signatures actuelles des menaces (cf. point 16.1, p. 231).

Il est conseillé de consulter régulièrement la liste des objets ; certains ne sont peut-être plus d'actualité tandis que d'autres peuvent être restaurés.

Une partie des services est orientée vers l'assistance pour l'utilisation du logiciel, par exemple :

- Le Service d'assistance technique offre une aide complète pour l'utilisation de Kaspersky Internet Security (cf. point 16.5, p. 256). Les experts de Kaspersky Lab ont tenté d'inclure tous les moyens possibles d'apporter cette assistance : assistance en ligne, forum de questions et de suggestions des utilisateurs, etc.
- Le service de notification des événements permet de configurer la notification aux utilisateurs des événements importants dans le fonctionnement de Kaspersky Internet Security (cf. point 16.10.1, p. 266). Il peut s'agir d'événements à caractère informatif ou d'erreurs qui nécessitent une réaction immédiate et dont il faut avoir conscience.
- L'autodéfense du logiciel et la restriction de l'accès protège les propres fichiers du logiciel contre les modifications réalisées par des personnes mal intentionnées, interdit l'administration externe du logiciel par des services et introduit des restrictions sur l'exécution de certaines actions à l'aide de Kaspersky Internet Security (cf. point □, p. 269). Par exemple, une modification du niveau de protection peut fortement influencer la sécurité des données sauvegardées sur votre ordinateur.

- Le service d'administration des clés de licence vous permet d'obtenir des informations complémentaires sur la licence utilisée, d'activer votre copie du logiciel et d'administrer les fichiers des clés de licence (cf. point **Error! Reference source not found.**, p. **Error! Bookmark not defined.**).

Le logiciel propose également une aide (cf. point 16.3.7, p. 246) détaillée et des rapports complets (cf. point 16.3, p. 237) sur le fonctionnement de tous les composants de la protection et l'exécution de toutes les tâches liées à la recherche de virus.

La constitution de la liste des ports permet de régler le contrôle des données qui transitent via les ports issues de certains composants de protection de Kaspersky Internet Security (cf. point 16.7, p. 259).

La création d'un disque de secours permet de ramener l'ordinateur à l'état antérieur à l'infection (cf. point 16.9, p. 263). Cela est particulièrement utile lorsqu'il n'est plus possible de lancer le système d'exploitation de l'ordinateur après l'infection du code malveillant.

Vous pouvez également modifier l'aspect extérieur de Kaspersky Internet Security et configurer les paramètre de l'interface actuelle (cf. point 16.8, p. 261).

Examinons en détails ces différents services.

16.1. Quarantaine pour les objets potentiellement infectés

La **quarantaine** est un dossier spécial dans lequel on retrouve les objets qui ont peut être été infectés par des virus.

Les **objets potentiellement infectés** sont des objets qui ont peut-être été infectés par des virus ou leur modification.

Pourquoi parle-t-on d'objets potentiellement infectés ? Il n'est pas toujours possible de définir si un objet est infecté ou non. Il peut s'agir des raisons suivantes :

- *Le code de l'objet analysé est semblable à celui d'une menace connue mais a été partiellement modifié*.

  Les signatures des menaces connues contiennent les menaces qui ont été étudiées par les experts de Kaspersky Lab. Si le programme malveillant a été modifié et que ces modifications ne figurent pas encore dans les signatures, Kaspersky Internet Security considère l'objet comme étant infecté par une modification d'un programme malveillant et le classe comme objet potentiellement infecté. Il indique obligatoirement à quelle menace cette infection ressemble.

- *Le code de l'objet infecté rappelle, par sa structure, celui d'un programme malveillant mais les signatures des menaces ne recensent rien de similaire*.

  Il est tout à fait possible qu'il s'agisse d'un nouveau type de virus et pour cette raison, Kaspersky Internet Security le classe comme un objet potentiellement infecté.

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

L'objet potentiellement infecté peut-être identifié et mis en quarantaine par l'antivirus de fichiers, l'antivirus de courrier électronique ou lors de la recherche de virus ou par la défense proactive.

Vous pouvez vous-même placer un objet en quarantaine en cliquant sur **Quarantaine** dans la notification spéciale qui apparaît à l'écran suite à la découverte d'un objet potentiellement infecté.

Lors d'une mise en quarantaine, le fichier est déplacé et non pas simplement copié : l'objet est supprimé du disque ou du message électronique et conservé dans le dossier de quarantaine. Les fichiers mis en quarantaine sont convertis dans un format spécial et ne représentent aucun danger.

16.1.1. Manipulation des objets en quarantaine

Le nombre total d'objets placés en quarantaine est repris dans les **Rapports** de la section **Service**. Dans la partie droite de la fenêtre principale, on retrouve le bloc spécial **Quarantaine** avec les informations suivantes :

- Le nombre d'objets potentiellement infectés découverts par Kaspersky Internet Security;
- La taille actuelle de la quarantaine.

Il est possible ici de supprimer tous les objets de la quarantaine à l'aide du bouton **Purger**. N'oubliez pas que cette action entraîne la suppression des objets du dossier de sauvegarde et des fichiers de rapport.

Pour manipuler les objets en quarantaine :

Cliquez avec le bouton gauche de la souris dans n'importe quelle partie du bloc **Quarantaine**.

Vous pouvez réaliser les opérations suivantes dans l'onglet quarantaine (cf. ill. 71) :

- Mettre en quarantaine un fichier que vous croyez être infecté par un virus et qui n'aurait pas été découvert par le logiciel. Cliquez pour ce faire sur **Ajouter** et sélectionnez le fichier souhaité. Il sera ajouté à la liste sous le signe *Ajouté par l'utilisateur*.

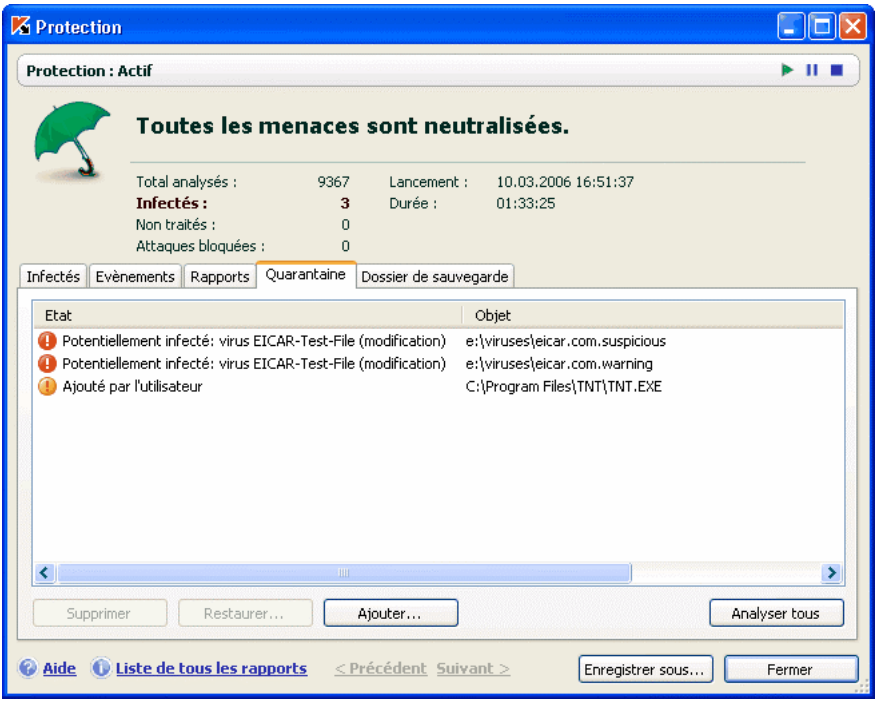


Illustration 71. Liste des objets en quarantaine

- Analyser et réparer à l'aide des signatures actuelles des menaces connues tous les objets potentiellement infectés qui se trouvent en quarantaine. Il suffit simplement de cliquer sur **Analyser tous**

  L'état de chaque objet en quarantaine après l'analyse et la réparation peut être soit *infecté*, *probablement infecté*, *fausse alerte, ok, etc*. Dans ce cas, un message de circonstance apparaît à l'écran et propose différents traitements possibles.

  L'état *infecté* signifie que l'objet est bien infecté mais qu'il n'a pas pu être réparé. Il est recommandé de supprimer de tels objets.

  Tous les objets dont l'état est qualifié de *fausse alerte* peuvent être restaurés sans crainte car leur état antérieur, à savoir *Probablement infecté* n'a pas été confirmé par le logiciel lors de la nouvelle analyse.

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

  Conseil

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

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

16.1.2. Configuration de la quarantaine

Vous pouvez configurer les paramètres de constitution et de fonctionnement de la quarantaine, à savoir :

- Définir le mode d'analyse automatique des objets en quarantaine après chaque mise à jour des signatures des menaces (pour de plus amples informations, consultez le point 15.3.4 à la page 229)

  Attention !

  Le logiciel ne peut analyser les objets en quarantaine directement après la mise à jour des signatures des menaces si vous utilisez la quarantaine à ce moment.

- Définir la durée de conservation maximum des objets en quarantaine.

  Par défaut, la durée de conservation des objets en quarantaine est fixée à 30 jours au terme desquels les objets sont supprimés. Vous pouvez modifier la durée de conservation des objets potentiellement infectés ou supprimer complètement cette limite.

  Pour ce faire :

  1. Ouvrez la fenêtre des paramètres de Kaspersky Internet Security en cliquant sur Configuration dans la fenêtre principale.
  2. Sélectionnez **Rapports** dans l'arborescence.

3. Définissez dans le bloc **Quarantaine et Dossier de sauvegarde** (cf. ill. 72) le délai de conservation au terme duquel les objets seront automatiquement supprimés.

Illustration 72. Configuration de la conservation des objets en quarantaine

16.2. Copie de sauvegarde des objets dangereux

Il n'est pas toujours possible de préserver l'intégrité des objets lors de la réparation. Si le fichier réparé contenait des informations importantes et que celles-ci ne sont plus accessibles (complètement ou partiellement) suite à la réparation, il est possible de le restaurer au départ de sa copie de sauvegarde.

La copie de sauvegarde est une copie de l'objet dangereux original qui est créée lors de la première réparation ou suppression de l'objet en question et qui est conservée dans le dossier de sauvegarde.

Le dossier de sauvegarde est un dossier spécial qui contient les copies des objets dangereux traités ou supprimés.
La fonction principale du dossier de sauvegarde est de permettre à n'importe quel moment la restauration de l'objet original.
Les fichiers placés dans le dossier de sauvegarde sont convertis dans un format spécial et ne représentent aucun danger.

16.2.1. Manipulation des copies de sauvegarde

Le nombre total de copies de sauvegarde placées dans le dossier est repris dans les **fichiers de données** de la section **Service**. Dans la partie droite de la fenêtre principale, on retrouve le bloc spécial **Dossier de sauvegarde** avec les informations suivantes :

- Le nombre de copies de sauvegarde créées par Kaspersky Internet Security;
- La taille actuelle du dossier.

Il est possible ici de supprimer toutes les copies du dossier à l'aide du bouton **Purger**. N'oubliez pas que cette action entraîne la suppression des objets du dossier de quarantaine et des fichiers de rapport.

Pour manipuler les copies des objets dangereux :

Cliquez avec le bouton gauche de la souris dans n'importe quelle partie du bloc **Dossier de sauvegarde**.

La partie centrale de l'onglet (cf. ill. 73) reprend la liste des copies de sauvegarde. Les informations suivantes sont fournies pour chaque copie : nom complet de l'objet avec chemin d'accès à son emplacement d'origine, l'état de l'objet attribué suite à l'analyse et sa taille.

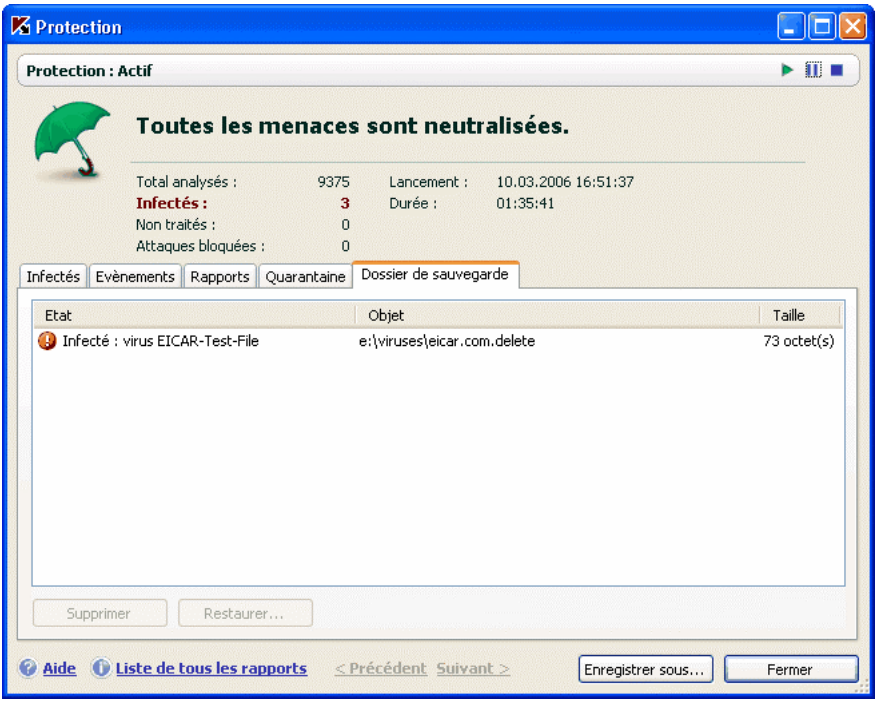


Illustration 73. Copies de sauvegarde des objets supprimés ou réparés

Vous pouvez restaurer les copies sélectionnées à l'aide du bouton **Restaurer**. L'objet est restauré au départ du dossier de sauvegarde avec le même nom qu'il avait avant la réparation.

Si l'emplacement d'origine contient un objet portant le même nom (cette situation est possible en cas de restauration d'un objet dont la copie avait été créée avant la réparation), l'avertissement de rigueur apparaîtra à l'écran. Vous pouvez modifier l'emplacement de l'objet restauré ainsi que son nom.

Nous vous recommandons de rechercher la présence d'éventuels virus directement après la restauration. Il sera peut-être possible de le réparer avec les signatures les plus récentes tout en préservant son intégrité.

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

Il est conseillé d'examiner fréquemment le contenu du dossier et de le nettoyer à l'aide du bouton **Supprimer**. Vous pouvez également configurer le logiciel afin qu'il supprime les copies les plus anciennes du répertoire (cf. point 16.2.2, p. 237).

16.2.2. Configuration des paramètres du dossier de sauvegarde

Vous pouvez définir la durée maximale de conservation des copies dans le dossier de sauvegarde.

Par défaut, la durée de conservation des copies des objets dangereux est fixée à 30 jours au terme desquels les copies sont supprimées. Vous pouvez modifier la durée de conservation maximale des copies ou supprimer complètement toute restriction. Pour ce faire :

1. Ouvrez la fenêtre des paramètres de Kaspersky Internet Security en cliquant sur Configuration dans la fenêtre principale.
2. Sélectionnez **Rapports** dans l'arborescence.
3. Définissez le délai de conservation des copies de sauvegarde dans le bloc **Quarantaine et Dossier de sauvegarde** (cf. ill. 72) dans la partie droite de la fenêtre.

16.3. Utilisation des rapports

Le fonctionnement de chaque composant de Kaspersky Internet Security et l'exécution de chaque tâche liée à la recherche de virus et à la mise à jour est consignée dans un rapport.

Le total des rapports composés par le logiciel en ce moment ainsi que leur taille totale (en octets) sont repris dans les **Rapports** de la section **Service** de la fenêtre principale du logiciel. Ces informations sont reprises dans le bloc **Rapports**.

Pour consulter les rapports :

Cliquez avec le bouton gauche de la souris dans n'importe quelle partie du bloc **Rapports**.

La fenêtre s'ouvre sur l'onglet **Rapports** (cf. ill. 74). Vous y verrez les derniers rapports sur tous les composants et les tâches antivirus lancées au cours de cette session de Kaspersky Internet Security. Le résultat du fonctionnement est affiché en regard de chaque composant ou tâche. Exemple, *interrompu(e)* ou *terminée.* Si vous souhaitez consulter l'historique complet des rapports pour la session en cours, cochez la case **Afficher l'historique des rapports**.

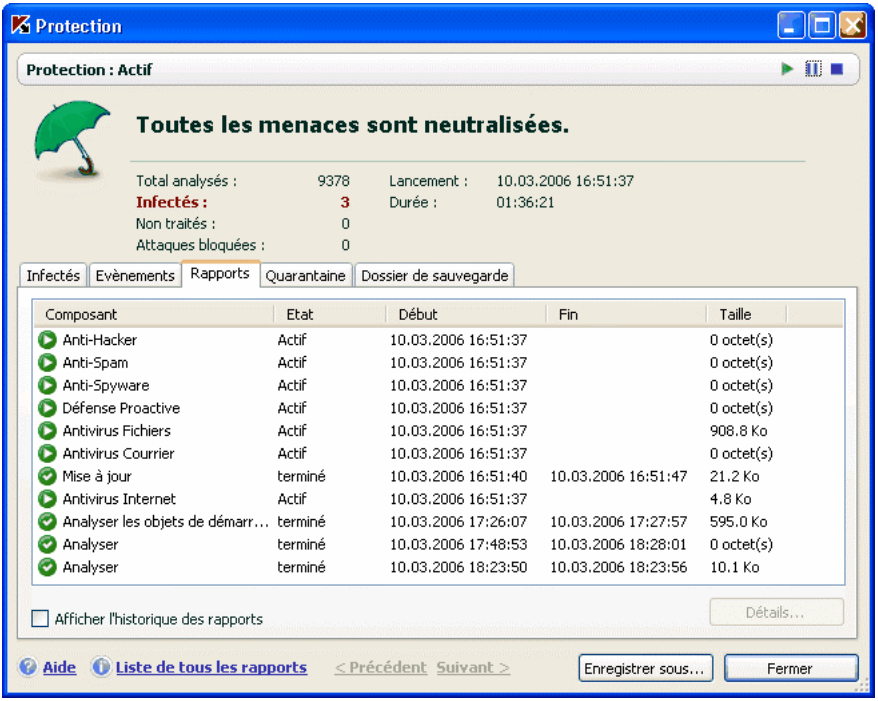


Illustration 74. Rapports sur le fonctionnement des composants du programme

Pour voir tous les événements consignés dans le rapport et relatifs au fonctionnement du composant ou à l'exécution d'une tâche :

sélectionnez le nom du composant ou de la tâche dans l'onglet **Rapports** et cliquez sur **Détails**.

Cette action entraîne l'ouverture d'une fenêtre contenant des informations détaillées sur le fonctionnement du composant ou de la tâche sélectionné. Les statistiques sont reprises dans la partie supérieure de la fenêtre tandis que les

détails apparaissent sur divers onglets de la partie centrale. En fonction du composant ou de la tâche, la composition des onglets peut varier:

- L'onglet **Infectés** contient la liste des objets dangereux découverts par le logiciel.
- **Evénements** illustre les événements survenus pendant l'exécution de la tâche ou le fonctionnement du composant
- L'onglet **Statistiques** reprend les statistiques détaillées de tous les objets analysés.
- L'onglet **Paramètres** reprend les paramètres qui définissent le fonctionnement du composant de protection, de la recherche de virus ou de la mise à jour des signatures des menaces.
- Les onglets **Macros** et **Registres** apparaissent uniquement dans le rapport de la défense proactive. Ils fournissent des informations sur toutes tentatives d'exécution de macros sur l'ordinateur et sur toutes les tentatives de modification de la base de registres système du système d'exploitation.
- Les onglets **Sites de phishing**, **Fenêtres pop up**, **Bannières** et **Tentatives de numérotation automatique** figurent uniquement dans le rapport d'Anti-Escroc. Ils contiennent des informations relatives à toutes les tentatives de phishing identifiées par le logiciel, ainsi que des renseignements sur toutes les fenêtres pop up, bannières et tentatives de numérotation automatique vers des sites payants bloquées .
- Les onglets **Attaques de réseau**, **Hôtes bloqués**, **Activités des applications** et **Filtrage des paquets** figurent uniquement dans le rapport d'Anti-Hacker. Ils proposent des informations sur toutes les attaques de réseau menées contre votre ordinateur et bloquées, ils contiennent une description de l'activité de réseau des applications concernées par les règles et de tous les paquets conforment aux règles de filtrage des paquets d'Anti-Hacker.
- Les onglets **Connexions établies**, **Ports ouverts** et **Trafic** définissent également l'activité de réseau de votre ordinateur. Ils représentent les connexions établies, les ports ouverts et le volume de données transmises ou reçues par l'ordinateur.

Tout le rapport peut être exporter dans un fichier au format texte. Cela peut-être utile lorsque vous ne parvenez pas à résoudre vous même un problème survenu pendant l'exécution d'une tâche ou le travail d'un composant et que vous devez vous adressez au service d'assistance technique . Vous devrez envoyer le rapport au format texte afin que nos experts puissent étudier le problème en profondeur et le résoudre le plus vite possible.

Pour exporter le rapport au format texte :

cliquez sur **Enregistrer sous** et indiquez où vous souhaitez enregistrer le fichier.

Lorsque vous en avez terminé avec le rapport, cliquez sur **Fermer**.

En plus des boutons **Paramètres** et **Statistiques**, ces onglets présentent également le bouton **Actions** que vous pouvez réaliser sur les objets de la liste. Ce bouton ouvre un menu contextuel qui reprend les points suivants (le contenu de la liste varie en fonction du rapport consulté; la liste ci-dessus est une énumération globale de tous ces points):

Réparer : tentative de réparation de l'objet dangereux. S'il est impossible de neutraliser l'objet, vous pouvez le lancer dans la liste en vue d'un traitement différé à l'aide des signatures des menaces actualisées ou le supprimer.

Supprimer de la liste : supprime l'objet de la liste.

Ajouter à la zone de confiance : ajoute l'objet en tant qu'exclusion de la protection. Ce choix entraîne l'ouverture de la fenêtre de la règle d'exclusion pour cet objet.

Réparer tous : neutralise tous les objets de la liste. Kaspersky Internet Security tente de traiter les objets à l'aide des signatures des menaces.

Purger : supprime le rapport sur les objets découverts. Tous les objets dangereux découverts demeurent sur l'ordinateur.

Afficher : ouvre Microsoft Windows Explorer au répertoire qui contient l'objet en question**.**

Consulter www.viruslist.com/fr : ouvre la description de l'objet dans l'Encyclopédie des virus sur le site de Kaspersky Lab.

Rechercher sur www.google.com : recherche d'informations relatives à l'objet à l'aide du moteur de recherche.

Rechercher : définit les termes de recherche des objets dans la liste en fonction du nom ou de l'état.

Vous pouvez également trier les informations présentées en ordre croissant ou décroissant pour chaque colonne.

16.3.1. Configuration des paramètres du rapport

Afin de configurer les paramètres de constitution et de conservation des rapports:

1. Ouvrez la boîte de dialogue de configuration de Kaspersky Internet Security en cliquant sur Configuration dans la fenêtre principale du logiciel.
2. Sélectionnez **Rapports** dans l'arborescence des paramètres.
3. Dans le bloc **Rapport** (cf. ill. 75), procédez à la configuration requise :
   - Consignez ou non les événements à caractère informatif. En règle générale, ces événements ne jouent pas un rôle crucial dans la protection. Afin de les consigner dans le rapport, cochez la case **Consigner les événements non critiques**;
   - Activez la conservation dans le rapport uniquement des événements survenus depuis le dernier lancement de la tâche. Cela permet de gagner de l'espace sur le disque en diminuant la taille du rapport. Si la case **Conserver uniquement les événements courants** est cochée, les informations reprises dans le rapport seront actualisées à chaque redémarrage de la tâche. Toutefois, seules les informations relatives aux événements non critiques seront écrasées.
   - Définissez le délai de conservation des rapports. Par défaut, ce délai est établi à 30 jours. Les rapports sont supprimés à l'issue des 30 jours. Vous pouvez modifier la durée de conservation des rapports ou ne pas imposer de limite.

Illustration 75. Configuration des paramètres de constitution des rapports

16.3.2. Onglet Infectés

Cet onglet (cf. ill. 76) contient la liste des objets dangereux découverts par Kaspersky Internet Security. Le nom complet et le statut attribué par le logiciel après l'analyse/le traitement est indiqué pour chaque objet.

Afin que la liste affiche, en plus des objets dangereux, les objets qui ont été réparés, cochez la case **Afficher les objets réparés**.

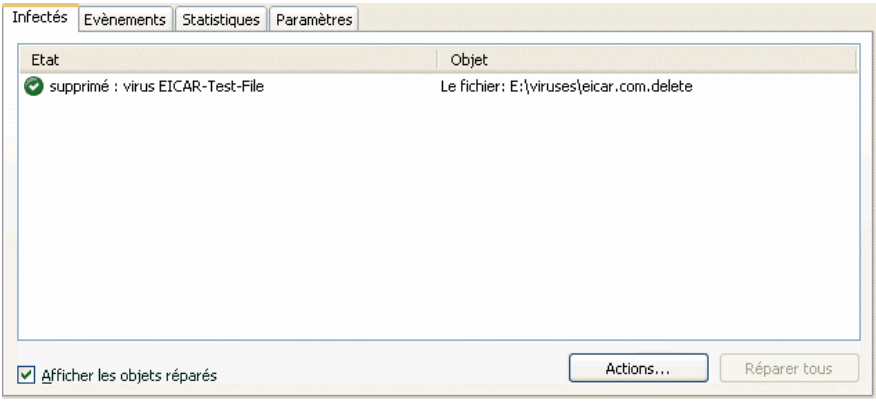


Illustration 76. Liste des objets dangereux découverts

16.3.3. Onglet Evénements

Cet onglet (cf. ill. 77) reprend la liste de tous les événements importants survenus pendant le fonctionnement du composant de protection, lors de l'exécution d'une tâche liée à la recherche de virus ou de la mise à jour des signatures des menaces, pour autant que ce comportement ne soit pas annulé par une règle de contrôle de l'activité (cf. point 10.1.1, p. 126).

Les événements prévus sont :

Evénements critiques. Evénements critiques qui indiquent un problème dans le fonctionnement du logiciel ou une vulnérabilité dans la protection de l'ordinateur. Exemple : *virus découvert, échec de fonctionnement*.

Evénements importants. Evénements auxquels il faut absolument prêter attention car ils indiquent une situation importante dans le fonctionnement du logiciel. Exemple : *interruption*.

Evénements informatifs. Evénements à caractère purement informatif qui ne contiennent aucune information cruciale. Exemple : *ok, non traité*. Ces événements sont repris dans le journal des événements uniquement si la case ☑ **Afficher les événements non critiques** est cochée.

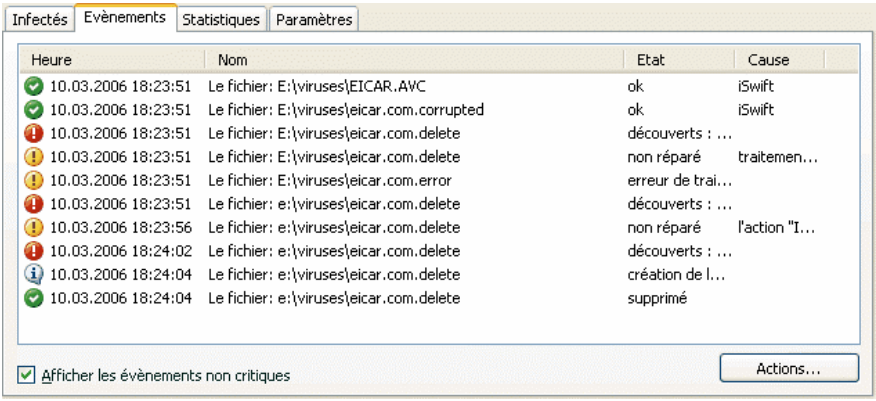


Illustration 77. Evénements survenus pendant

Le format de présentation de l'événement dans le journal des événements peut varier en fonction du composant ou de la tâche. Ainsi, pour la mise à jour, les informations reprises sont :

- Le nom de l'événement;
- Le nom de l'objet pour lequel cet événement a été consigné;
- L'heure à laquelle l'événement est survenu;
- La taille du fichier téléchargé.

Pour les tâches liées à la recherche de virus, le journal des événements contient le nom de l'objet analysé et le statut attribué à l'objet suite à l'analyse/au traitement.

Vous pouvez également entraîner Anti-Spam à l'aide à l'aide d'un menu contextuel lors de la consultation du rapport en question. Pour ce faire, ouvrez le menu contextuel et sélectionnez **Marquer comme courrier indésirable** s'il s'agit d'un message non sollicité ou **Marquer comme courrier normal** s'il s'agit d'un message utile. De plus, sur la base des informations obtenues pendant l'analyse du message, vous pouvez enrichir les listes "blanche" et "noire" d'Anti-Spam. Pour ce faire, utilisez les points adéquats du menu contextuel.

16.3.4. Onglet Statistiques

Cet onglet reprend les statistiques détaillées du fonctionnement du logiciel ou de l'exécution des tâches liées à la recherche de virus (cf. ill. 78). Vous pouvez voir :

- Le nombre d'objets soumis à l'analyse antivirus pendant la session actuelle du composant ou lors de l'exécution de la tâche. Ce chiffre reprend le nombre d'archives, de fichiers compactés, de fichiers protégés par un mot de passe et d'objets corrompus analysés.
- Le nombre d'objets dangereux découverts, le nombre d'entre eux qui n'a pas pu être réparés, le nombre supprimés et le nombre mis en quarantaine.

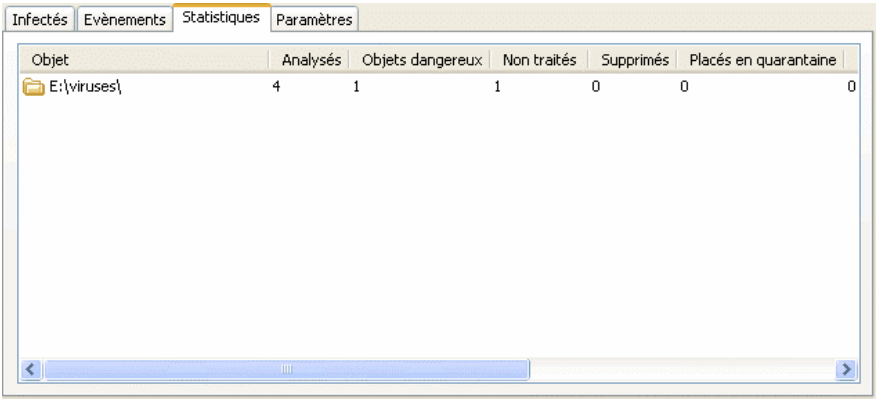


Illustration 78. Statistique du composant

16.3.5. Onglet Paramètres

Cet onglet (cf. ill. 79) présente tous les paramètres qui définissent le fonctionnement du composant ou l'exécution des tâches liées à la recherche de virus ou à la mise à jour. Vous pouvez voir le niveau de protection offert par le composant ou le niveau de protection défini pour la recherche de virus, les actions exécutées sur les objets dangereux, les paramètres appliqués à la mise à jour, etc. Pour passer à la configuration des paramètres, cliquez sur Modifier les paramètres.

Pour la recherche de virus, vous pouvez configurer des conditions complémentaires d'exécution :

- Etablir la priorité d'exécution d'une tâche d'analyse en cas de charge du processeur. Par défaut, la case ☑ **Suspendre l'analyse si le processeur est occupé par d'autres applications** est cochée. Le programme surveille la charge du processeur et des sous-système des disques pour déceler l'activité d'autres applications. i l'activité augmente sensiblement et gêne le fonctionnement normal de l'application de l'utilisateur, le programme réduit l'activité liée à l'analyse. Cela se traduit

par une augmentation de la durée de l'analyse et le transfert des ressources aux applications de l'utilisateur.

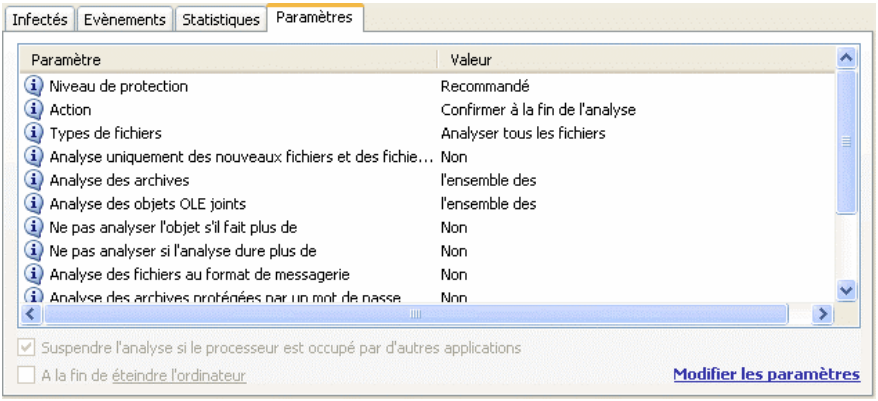


Illustration 79. Paramètres de fonctionnement du composant

- Définir le mode de fonctionnement de l'ordinateur après la recherche de virus. Vous pouvez configurer la désactivation/le redémarrage de l'ordinateur ou le passage en mode de veille. Pour opérer votre choix, cliquez avec le bouton gauche de la souris sur le lien jusqu'à ce qu'il prenne la valeur voulue.

  Cette option est utile si vous lancez la recherche de virus à la fin de votre journée de travail et que vous ne voulez pas attendre la fin de l'analyse.

  Cependant, l'utilisation de ce paramètre requiert le préparatif suivant : le cas échéant, il faut, avant de lancer l'analyse, désactiver la requête du mot de passe lors de l'analyse des objets et sélectionner le mode de traitement automatique des objets dangereux. Le mode de fonctionnement interactif est désactivé suite à ces actions. Le programme n'affichera aucune requête susceptibles d'interrompre l'analyse.

16.3.6. Onglet *Macros*

Toutes les macros que le système a tenté d'exécuter pendant la séance actuelle de Kaspersky Internet Security sont reprises sur l'onglet **Macros** (cf. ill. 80). Le rapport reprend le nom complet de chaque macro, l'heure de l'exécution et l'état suite au traitement de la macro.

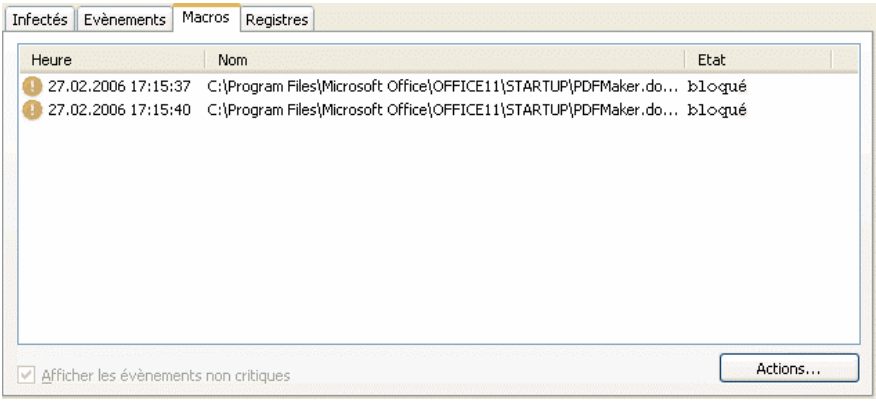


Illustration 80. Liste des macros dangereuses découvertes

Vous pouvez définir les événements que vous souhaitez voir sur cet onglet du rapport. Pour annuler la consultation des informations, désélectionnez la case **Afficher les événements non critiques**.

16.3.7. Onglet *Registre*

Les opérations sur les clés de la base de registres système au moment du lancement du programme sont consignées dans l'onglet **Registre** (cf. ill. 81), si l'enregistrement n'est pas contraire à la règle (cf. point 10.1.4.2, p. 138).

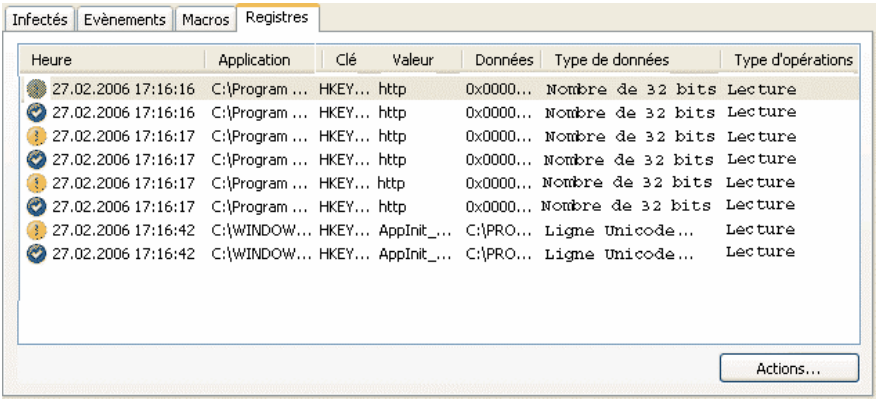


Illustration 81. Lecture et modification de clés de la base de registre

L'onglet reprend le nom complet de la clé, sa valeur, le type de données ainsi que des renseignements sur l'opération exécutée : tentative d'exécution d'une action quelconque, heure de l'autorisation, etc..

16.3.8. Onglet *Sites de phishing*

Cet onglet du rapport (cf. ill. 82) reprend toutes les tentatives d'attaques de phishing réalisées durant la session actuelle de Kaspersky Internet Security. Le rapport reprend le lien vers le site fictif découvert dans le message, le chat ou tout autre moyen, la date et l'heure de l'identification de l'attaque et son état : bloquée ou non.

Illustration 82. Tentatives de blocage d'attaques de phishing

16.3.9. Onglet *Fenêtres pop up*

Les adresses de toutes les fenêtres pop up bloquées par Anti-Escroc figurent sur cet onglet du rapport (cf. ill. 83). En règle générale, ces fenêtres s'ouvrent dans des sites Web.

Chaque fenêtre pop up est accompagnée de son adresse Internet et de la date et de l'heure a laquelle elle a été bloquée.

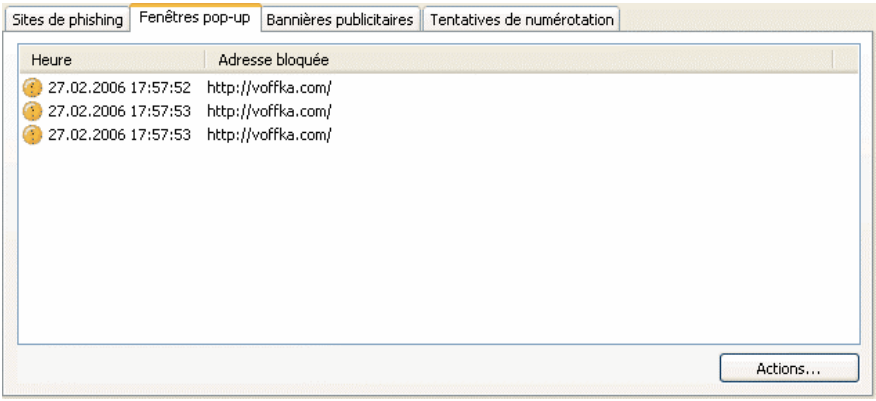


Illustration 83. Liste des fenêtres pop up bloquées

16.3.10. Onglet *Bannières publicitaires*

Les adresses des bannières découvertes dans la session en cours de Kaspersky Internet Security sont reprises sur cet onglet du rapport (cf. ill. 84). Chaque bannière est définie par son adresse Internet et le résultat de son traitement : autorisée ou non.

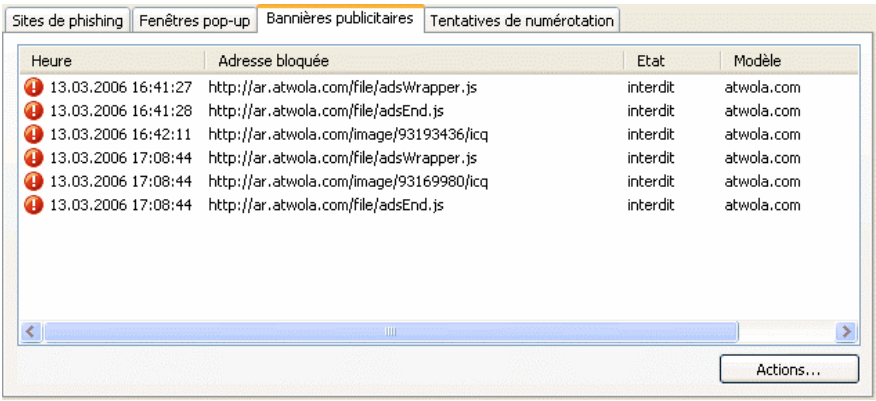


Illustration 84. Liste des bannières bloquées

Vous pouvez autoriser l'affichage des bannières interdites. Pour ce faire, sélectionnez l'objet voulu dans la liste et cliquez sur **Action** → **Autoriser**.

16.3.11. Onglet *Tentative de numérotation*

Cet onglet (cf. ill. 85) reprend toutes les tentatives de connexions cachées vers des sites Internet payant. En règle générale, ces tentatives sont menées par des applications malicieuses installées sur votre ordinateur.

Le rapport vous permet de voir le module à l'origine de la tentative de numérotation, le numéro utilisée et l'état de cette tentative : bloquée ou autorisée et pour quelles raisons.

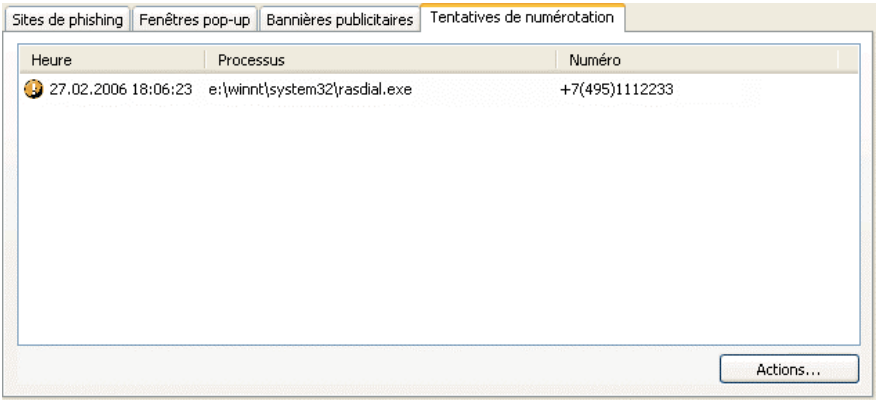


Illustration 85. Tentatives de numérotations automatiques vers un site payant

16.3.12. Onglet *Attaques de réseau*

Cet onglet (cf. ill. 86) présente une brève description des attaques de réseau qui ont été menées contre votre ordinateur. Ces informations sont consignées si le système de détection d'intrusions, qui surveille toutes les tentatives d'attaques contre votre ordinateur, est activé.

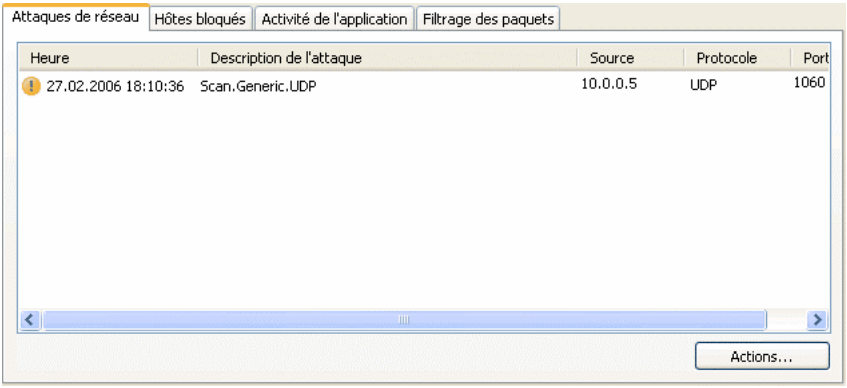


Illustration 86. Liste des attaques de réseau bloquées

L'onglet *Attaques de réseau* reprend les informations relatives à l'attaque :

- Source de l'attaque. Il peut s'agir d'une adresse IP, de l'hôte, etc..
- Le numéro du port local qui a été la proie de la tentative d'attaque.
- Une brève description de l'attaque.
- L'heure à laquelle la tentative d'attaque a été réalisée.

16.3.13. Onglet *Hôtes bloqués*

Tous les hôtes dont l'activité de réseau a été bloquée suite à la découverte de l'attaque sont repris sur cet onglet (cf. ill. 87).

Chaque hôte est accompagné de son nom et de l'heure à laquelle il a été bloqué. Vous pouvez débloquer l'hôte au départ de ce même onglet. Pour ce faire, sélectionnez l'hôte dans la liste et cliquez sur **Actions → Débloquer**.

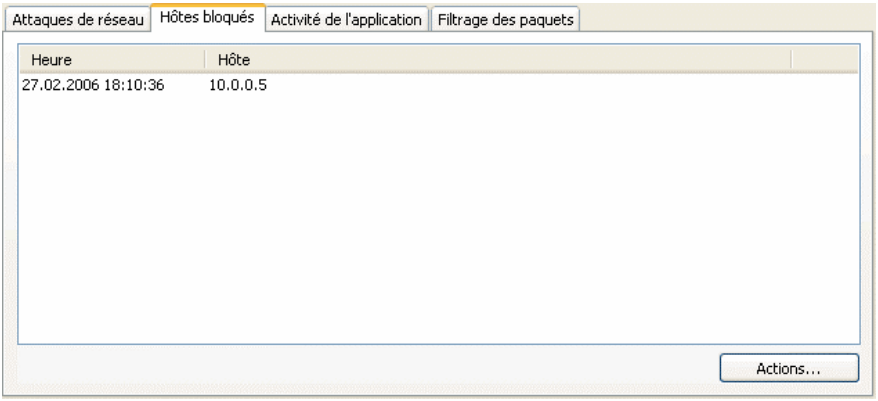


Illustration 87. Liste des hôtes bloqués

16.3.14. Onglet *Activité de l'application*

Si le Pare-feu est utilisé par Kaspersky Internet Security, toutes les applications dont l'activité tombe sous le coup de la règle pour l'application et a été identifiée au cours de la session actuelle, sont reprises sur l'onglet **Activité de l'application** (cf. ill. 88).

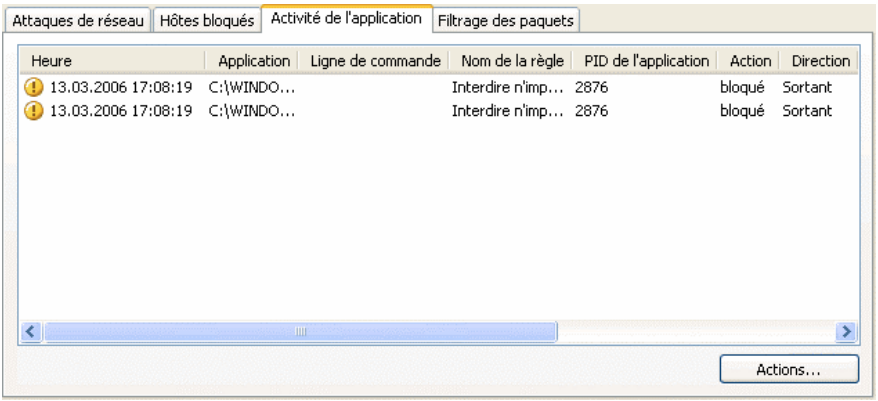


Illustration 88. Activité contrôlée de l'application

L'activité est enregistrée uniquement si la case **Consigner dans le rapport**. est cochée dans la règle. C'est le cas pour les règles pour les applications livrées avec Kaspersky Internet Security.

Pour chaque application, vous pouvez voir ses principales propriétés (nom, PID et nom de la règle) et une brève description de son activité (protocole, direction du paquet, etc.). L'onglet indique également si l'activité de l'application a été bloquée ou non.

16.3.15. Onglet *Filtrage des paquets*

Tous les paquets dont l'envoi et la réception tombent sous le coup d'une règle de filtrage des paquets enregistrées dans la session de Kaspersky Internet Security sont repris sur l'onglet **Filtrage des paquets** (cf. Illustration 89).

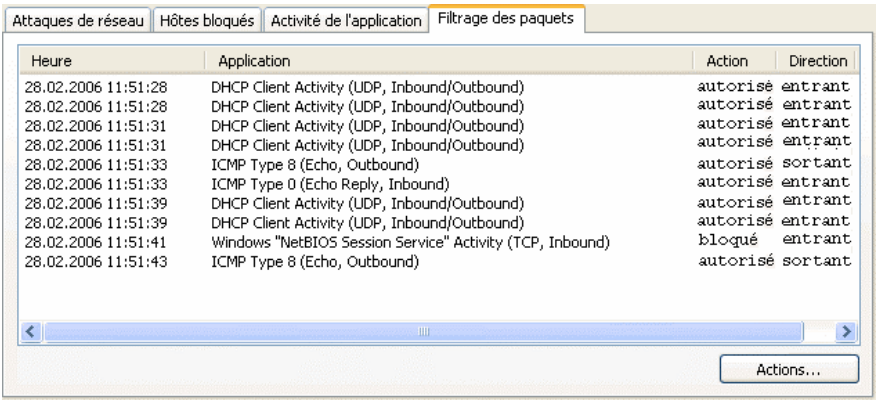


Illustration 89. Paquets de données contrôlés

L'activité est enregistrée uniquement si la case **Consigner dans le rapport**. est cochée dans la règle. C'est le cas pour les règles pour les applications livrées avec Kaspersky Internet Security.

Chaque paquet est accompagné du nom de l'application qui a lancé le transfert ou la réception, le résultat du filtrage (bloqué ou non), la direction du paquet, le protocole et d'autres paramètres de la connexion de réseau pour la réception et le transfert du paquet.

16.3.16. Onglet *Connexions établies*

Toutes les connexions actives établies sur votre ordinateur à l'instant figurent sur l'onglet **Connexions établies** (cf. ill. 90). Pour chacune de ces connexions, vous pouvez voir le nom de l'application qui l'a ouverte, le protocole utilisée, le sens de la connexion (entrante ou sortante) et les paramètres de la connexion (ports

local et distant et adresse IP). Vous pouvez voir également la durée de la connexion et le volume de données reçues/transmises. Vous pouvez créer une règle pour la connexion sélectionnée ou vous pouvez l'interrompre. Pour ce faire, utilisez les points correspondants du menu contextuel que vous pouvez ouvrir à l'aide d'un clic du bouton droit de la souris dans la liste des rapports.

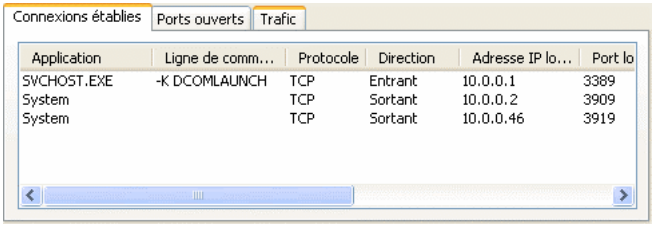


Illustration 90. Liste des connexions établies

16.3.17. Onglet *Ports ouverts*

Tous les ports ouverts en ce moment sur votre ordinateur pour les connexions de réseau sont repris sur l'onglet **Ports ouverts** (cf. ill. 91). Pour chaque port, vous retrouvez son numéro, le protocole de transfert des données, le nom de l'application qui utilise le port ainsi que la période pendant laquelle le port a été ouvert pour la connexion.

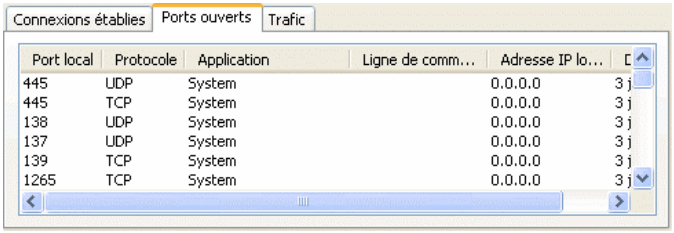


Illustration 91. Liste des ports ouverts sur l'ordinateur

Ces informations peuvent s'avérer utiles en cas d'épidémies et d'attaques de réseau par exemple lorsque l'on connaît le port vulnérable. Vous pouvez voir si ce port est ouvert sur votre ordinateur et prendre les mesures qui s'imposent pour protéger votre ordinateur (par exemple, activer le Détecteur d'attaques, fermer le port vulnérable ou créer une règle pour celui-ci).

16.3.18. Onglet *Trafic*

Cet onglet (cf. ill. 92) reprend les informations relatives à toutes les connexions entrantes et sortantes établies entre votre ordinateur et d'autres ordinateurs (y compris des serveurs Web, des serveurs de messagerie, etc.). Les informations suivantes sont reprises pour chaque connexion : nom et adresse IP de l'hôte avec lequel la connexion est établie ainsi que le volume du trafic entrant et sortant.

Illustration 92. Trafic sur les connexions établies

16.4. Informations générales sur le logiciel

La section **Service** de la fenêtre principale affiche des informations générales sur le logiciel (cf. ill. 93).

Illustration 93. Informations relatives au logiciel, à la licence et au système sur lequel il est installé

Ces informations sont scindées en trois blocs :

- La section **Informations relatives au logiciel** affiche la version du logiciel, la date de la dernière mise à jour et la quantité de menaces connues à ce moment.
- La section **Informations relatives à la licence** fournit des informations sur votre licence d'utilisation de Kaspersky Internet Security.
- Le bloc **Informations relatives au système** reprend de brèves informations sur le système d'exploitation installé sur votre ordinateur.

Toutes ces informations sont nécessaires lors des contacts avec le service d'Assistance technique de Kaspersky Lab (cf. point 16.5, p. 256).

16.5. Prolongation de la licence

Kaspersky Internet Security fonctionne grâce à une *licence*. Elle est octroyée sur la base du code d'activation et vous donne le droit d'utiliser celui-ci dès le jour de l'acquisition et de l'activation de la clé.

Une fois la licence expirée, le logiciel continue à fonctionner, si ce n'est qu'il ne sera plus possible de mettra à jour les signatures des menaces. Vous pourrez toujours analyser votre ordinateur à l'aide de la recherche de virus et utiliser les composants de la protection, mais uniquement sur la base des signatures des menaces 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 licence d'utilisation de Kaspersky Internet Security. Deux semaines avant la date d'expiration, le programme vous avertira. Au cours des deux semaines suivantes, le programme affichera à chaque démarrage le message de circonstance.

Afin de renouveler la licence, vous devez absolument obtenir un nouveau code d'activation. Pour ce faire :

1. Contactez le distributeur chez lequel vous avez acheté le logiciel.

ou:

Achetez un code d'activation directement chez Kaspersky Lab en cliquant sur le lien Acheter une licence (cf. Illustration 94) dans la partie gauche de l'onglet **Assistance technique** ou en cliquant **Renouveler** dans la boîte de dialogue **Gestion des clés de licence**. Remplissez le formulaire requis sur notre site Internet. Une fois le paiement effectué, vous recevrez à l'adresse électronique spécifiée le code d'activation.

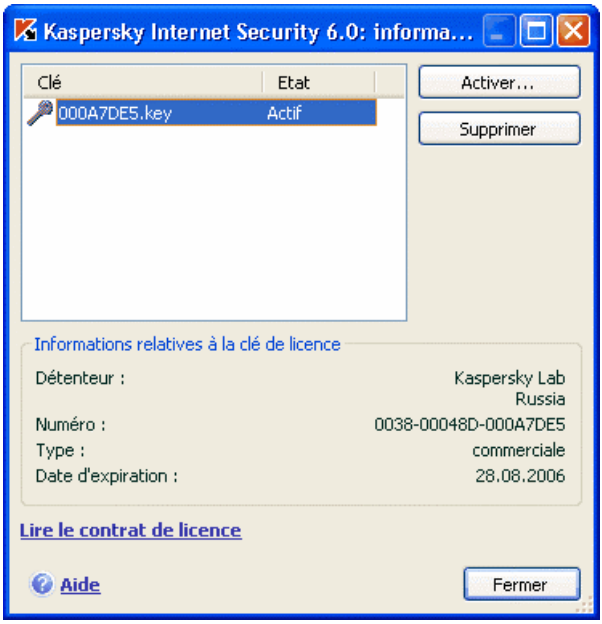


Illustration 94. Informations relatives à la licence

2. Activez le programme à l'aide du code d'activation. Pour ce faire :

   a. Sélectionnez la section **Services** dans la fenêtre principale du programme et cliquez avec le bouton gauche de la souris dans n'importe quel endroit du bloc **Informations relatives à la licence**.

   b. Si vous souhaitez prolonger la licence à l'aide d'une clé de licence, cliquez sur **Ajouter** dans la fenêtre **Informations relatives à la licence** et sélectionnez la nouvelle clé dans la boîte de dialogue traditionnelle de sélection de fichiers.

   c. Si vous possédez un code d'activation, cliquez sur **Activer** dans la boîte de dialogue d'administration des licences et activez le programme à l'aide de l'Assistant.

16.6. Service d'assistance technique aux utilisateurs

Kaspersky Internet Security vous offre un large éventail de possibilités pour régler les problèmes et les questions liées à l'utilisation du logiciel. Ils sont tous repris sous **Assistance technique** (cf. ill. 95) dans la section **Service**.

Illustration 95. Informations relatives à l'assistance technique

En fonction du problème que vous voulez résoudre, nous vous proposons plusieurs services :

Questions fréquement posées. Il s'agit également d'une rubrique distincte du site Web de Kaspersky Lab qui contient les recommandations du service d'assistance technique sur l'utilisation des produits de Kaspersky Lab ainsi que les réponses aux questions fréquemment posées.
Site internet : http://kb.kaspersky.fr

Assistance Technique en ligne. Cette solution permet une approche pas à pas de la définitions du souci rencontré afin de vous offrir la solution adequate.

Site internet : http://case.kaspersky.fr

Site du Support Technique. Ce site regroupe toutes les informations concernant les outils d'information vous permettant de nous contacter par téléphone ou par email, vous y trouverez aussi des sites associés, des données sur les mises à jour, etc...

Site internet : http://support.kaspersky.fr

16.7. Constitution de la liste des ports contrôlés

Les composants tels que l'antivirus de courrier électronique, l'antivirus Internet, l'Anti-Escroc et l'anti-spam contrôlent les flux de données transmis par des protocoles définis et qui transitent par certains ports ouverts de l'ordinateur. Ainsi, l'antivirus de courrier électronique analyse les données transmises via le protocole SMTP tandis que l'antivirus Internet analyse les paquets HTTP.

La lise des ports qui sont normalement utilisés pour le courrier et le trafic http sont repris dans le logiciel. Vous pouvez ajouter de nouveaux ports ou désactiver le contrôle exercé sur certains ports, ce qui suspend la recherche d'éventuels objets dangereux dans le trafic qui transite via ces ports.

Pour modifier la liste des ports soumis à un contrôle :

1. Ouvrez la boîte de dialogue de configuration de Kaspersky Internet Security en cliquant sur le lien Configuration de la fenêtre principale.
2. Sélectionnez **Configuration du réseau** dans le groupe **Service** de l'arborescence des paramètres du logiciel.
3. Dans la partie droite de la fenêtre de configuration, cliquez sur **Configuration des ports**.
4. Modifiez la liste des ports soumis à un contrôle dans la fenêtre qui s'ouvre(cf. ill. 96).

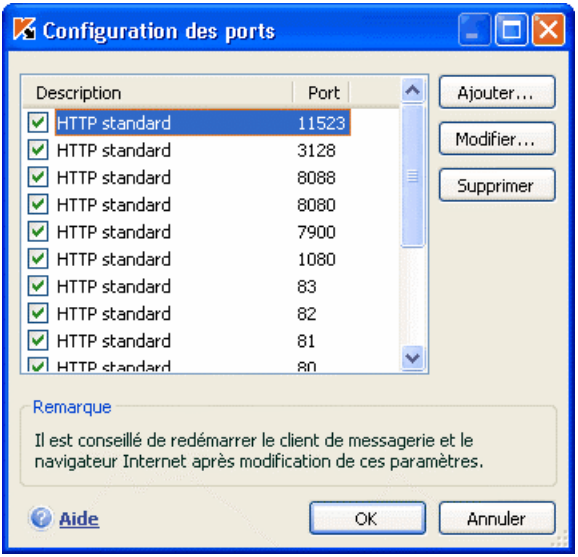


Illustration 96. Liste des ports contrôlés

Pour ajouter un nouveau port à la liste :

1. Cliquez sur **Ajouter** dans la fenêtre de configuration des ports.
2. Saisissez le numéro du port et sa description dans les champs correspondant de la fenêtre **Nouveau port**.

Par exemple, votre ordinateur possède un port inhabituel pour l'échange des données avec un ordinateur distant via le protocole HTTP. C'est l'antivirus Internet qui est chargé du contrôle du trafic HTTP. Afin de pouvoir rechercher la présence éventuelle de code malveillant dans ces données, il faudra ajouter ce port à la liste des ports soumis à un contrôle.

Lors du lancement de n'importe quel composant de Kaspersky Internet Security, le port 1110 est ouvert pour écouter toutes les connexions entrantes. Si ce port est occupé par une autre application, le port 1111, 1112, etc. sera choisi pour l'écoute.

Si vous utilisez simultanément Kaspersky Internet Security et un pare-feu d'un autre éditeur, il faudra configurer ce pare-feu pour qu'il autorise le processus *avp.exe* (processus interne de Kaspersky Internet Security) sur tous les ports cités

Par exemple, votre pare-feu possède une règle pour *iexplorer.exe* qui permet à ce processus d'établir une connexion sur le port 80.

Cependant Kaspersky Internet Security qui intercepte la requête de connexion lancée par *iexplorer.exe* sur le port 80 la transmet à son processus *avp.exe* qui tente, à son tour, d'établir une connexion avec la page Web demandée. Si aucune règle d'autorisation n'a été définie pour le processus *avp.exe*, le pare-feu bloquera la requête. Par conséquent, l'utilisateur ne pourra pas ouvrir la page Web.

16.8. Configuration de l'interface de Kaspersky Internet Security

Kaspersky Internet Security vous permet de modifier l'aspect extérieur du logiciel à l'aide de divers éléments graphiques et d'une palette de couleurs. Il est également possible de configurer l'utilisation des éléments actifs de l'interface tels que l'icône de l'application dans la barre des tâches et les infobulles.

Pour configurer l'interface du logiciel :

1. Ouvrez la boîte de dialogue de configuration de Kaspersky Internet Security à l'aide du lien Configuration de la fenêtre principale.
2. Sélectionnez **Apparence** dans le groupe **Service** de l'arborescence des paramètres du logiciel (cf. ill. 97).

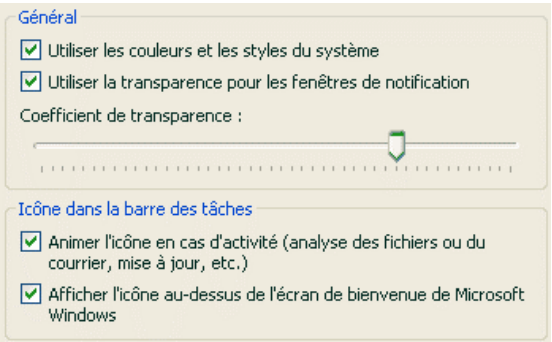


Illustration 97. Configuration de l'interface du programme

Dans la partie droite de la fenêtre des paramètres, vous pouvez décider d':

- Afficher ou non l'indicateur de la protection de Kaspersky Internet Security lors du démarrage du système d'exploitation.

  Par défaut, cet indicateur apparaît dans le coin supérieur droit de l'écran au moment du démarrage du logiciel. Il indique que la protection de l'ordinateur contre n'importe quelle menace est activée. Si vous ne

souhaitez pas afficher l'indicateur de protection, désélectionnez la case **Afficher l'icône au-dessus de l'écran de bienvenue de Microsoft Windows**.

- Animer ou nom l'icône de l'application dans la barre des tâches.

  L'icône de l'application dans la barre des tâches varie en fonction de l'opération exécutée. Par exemple, lors de l'analyse d'un script, une image représentant un script apparaît sur le fond de l'icône. Une image représentant une lettre apparaît pendant l'analyse du courrier. L'icône est animée par défaut. Si vous ne souhaitez pas utiliser l'animation, désélectionnez la case **Animer l'icône en cas d'activité**. Dans ce cas, l'icône indiquera uniquement l'état de la protection de votre ordinateur. Lorsque la protection est activée, l'icône est en couleur. Lorsque la protection est suspendue ou désactivée, l'icône apparaît est grisée.

- Degré de transparence des infobulles.

  Toutes les opérations de Kaspersky Internet Security au sujet desquelles vous devez être alerté immédiatement ou qui nécessitent une prise de décision rapide sont annoncées sous la forme d'une infobulle qui apparaît au-dessus de l'icône de l'application dans la barre des tâches. Ces infobulles sont transparentes afin de ne pas vous perturber dans votre travail. Le fond de l'infobulle devient solide dès que vous placer le curseur de la souris sur la fenêtre. Il est possible de modifier le degré de transparence de ces infobulles. Pour ce faire, faites glisser le curseur de l'échelle **Coefficient de transparence** jusqu'au niveau requis. Afin de supprimer la transparence des messages, désélectionnez la case **Utiliser la transparence pour les fenêtres de notification**.

- Utilisation d'éléments graphiques propres et de la palette des de couleurs dans l'interface du logiciel.

  Toutes les couleurs, polices de caractères, images et textes utilisés dans l'interface de Kaspersky Internet Security peuvent être modifiés. Vous pouvez créer votre propre environnement graphique pour le logiciel, localiser l'interface dans la langue de votre choix. Pour activer votre propre environnement graphique, indiquez le répertoire avec ses paramètres dans le champ **Répertoire avec la description des "Skins"**. Cliquez sur **Parcourir** pour sélectionner le répertoire

  Les couleurs et les styles du système sont utilisés par défaut. Si vous souhaitez en utiliser d'autres, désélectionnez la case **Utiliser les couleurs et les styles du système**. Dans ce cas, le système utilisera les styles que vous aurez indiqués lors de la configuration de l'environnement graphique.

N'oubliez pas que la configuration personnalisée de l'interface de Kaspersky Internet Security n'est pas préservée lors du rétablissement des paramètres par défaut ou de la suppression du programme.

16.9. Disque de secours

Kaspersky Internet Security propose la création d'un disque de secours.

Le disque de secours doit permettre la restauration des fonctions du système après une attaque de virus qui aurait endommagé le système de fichiers du système d'exploitation et qui rendrait impossible le chargement initial. Le disque comprend :

- Les fichiers systèmes de Microsoft Windows XP Service Pack 2;
- Un ensemble d'utilitaire pour le diagnostic du système d'exploitation;
- Les fichiers du logiciel Kaspersky Internet Security;
- Les fichiers contenant les signatures des menaces.

Afin de créer le disque de secours:

1. Ouvrez la fenêtre principale du logiciel et sélectionnez **Disque de secours** dans la section **Service**.
2. Cliquez sur **Lancement de l'Assistant** afin de lancer la création du disque de secours.

16.9.1. Création d'un disque de secours de restauration

Attention ! Afin de pouvoir créer ce disque de secours, vous devrez utiliser le disque d'installation de Microsoft Windows XP Service Pack 2.

La création d'un disque de secours s'opère à l'aide du programme spécial PE Builder.

Afin de créer un disque de secours à l'aide de PE Builder, il faut tout d'abord l'installer sur l'ordinateur.

De plus, lors de l'utilisation de PE Builder, il est indispensable de lancer une fois le logiciel à l'aide de la commande **Démarrer → Programmes → PE Builder** après son installation.

La création du disque de secours s'opère à l'aide d'un assistant spécial qui contient une succession de fenêtre (étape) entre lesquelles vous pouvez naviguer à l'aide des boutons **Précédent** et **Suivant**. Pour terminer le travail de l'assistant, cliquez sur **Terminer**. Pour arrêter l'Assistant à n'importe quelle étape, cliquez sur **Annuler**.

Etape 1. Préparatifs pour l'enregistrement

Si vous avez décidé à l'étape précédente de créer le disque à l'aide d'un programme spécial, indiquez le chemin d'accès aux répertoires suivants :

- Répertoire d'installation de PE Builder.
- Répertoire de sauvegarde des fichiers du disque de secours avant la création du cédérom.

  Si ce n'est pas la première fois que vous créez un disque de secours, ce répertoire contient déjà l'ensemble des fichiers préparés la dernière fois. Afin d'utiliser les fichiers enregistrés préalablement, cochez la case adéquate.

  N'oubliez pas que la version antérieure des fichiers du disque de secours contient les anciennes signatures des menaces. Afin de garantir la meilleure recherche de virus et la restauration du système, il est conseillé d'actualiser les signatures des menaces et de créer une nouvelle version du disque de secours.

- Cédérom d'installation de Microsoft Windows XP Service Pack 2.

Cliquez sur **Suivant** une fois que vous aurez saisi le chemin d'accès aux différents répertoires. Cette action entraînera le lancement de PE Builder et la création des fichiers du disque de secours. Attendez la fin du processus. Cela peut durer quelques minutes.

Etape 2. Création d'un fichier ISO

Une fois que PE Builder aura terminé de créer les fichiers du disque de secours, la fenêtre **Création d'un fichier ISO** s'ouvrira.

Le fichier ISO est une image du futur disque de secours sous la forme d'une archive. Les fichiers au format ISO sont correctement interprétés par la majorité des programmes d'enregistrement de cédérom (par exemple, Nero).

S'il ne s'agit pas du premier disque de secours que vous créez, vous pouvez utiliser le fichier ISO de la version précédente. Pour ce faire, sélectionnez **Fichier ISO existant**.

Etape 3. Enregistrement du disque

Cette fenêtre de l'Assistant vous permet de choisir quand enregistrer les fichiers du disque de secours sur le cédérom : maintenant ou plus tard.

Si vous avez sélectionné l'enregistrement immédiat du disque, indiquez s'il faut nettoyer le contenu du lecteur de cédérom avant de procéder à l'enregistrement. Pour ce faire, cochez la case correspondante. Cette possibilité est accessible uniquement si le graveur de cédérom est compatible avec les cédéroms réinscriptibles.

En cliquant sur **Suivant**, vous lancez le processus d'enregistrement du cédérom de démarrage. Attendez la fin du processus. Cela peut durer quelques minutes.

Etape 4. Fin de la création du disque de secours

Cette fenêtre de l'assistant vous informe de la réussite de la création du disque de secours.

16.9.2. Utilisation du disque de secours

Lorsqu'il n'est plus possible de démarrer le système d'exploitation suite à une attaque de virus, agissez comme suit :

1. Créez un disque de secours à l'aide de Kaspersky Internet Security sur l'ordinateur sain.
2. Introduisez le disque de secours dans le lecteur de l'ordinateur infecté et redémarrez. Cette action entraîne le lancement du système d'exploitation Microsoft Windows XP SP2 avec l'interface du logiciel Bart PE.
   Le logiciel Bart PE prend en charge le fonctionnement dans un réseau local. Lors du lancement du programme, l'écran affiche une requête d'activation de la prise en charge de l'utilisation au sein de réseau local. Acceptez-la si vous avez l'intention d'actualiser les bases des signatures des virus depuis un répertoire local avant d'analyser l'ordinateur. Si la mise à jour n'est pas nécessaire, annulez l'activation de la prise en charge du réseau.
3. Pour lancer Kaspersky Internet Security, exécutez la commande **Démarrer→Programmess→Kaspersky Internet Security 6.0→Start**.

   Cette action entraîne l'ouverture de la fenêtre principale de Kaspersky Internet Security. En mode de restauration, seules la recherche de virus et la mise à jour des signatures des menaces au départ du réseau local (si vous avez activé la prise en charge du réseau dans Bart PE) sont accessibles.

4. Lancez l'analyse antivirus de l'ordinateur. Le rapport reprenant le résultat de l'analyse ainsi que les objets placés en quarantaine ou dan le dossier de sauvegarde sera enregistré dans le répertoire *C:\AVP6_TEMP*.

En mode de réparation, Kaspersky Internet Security fonctionnera uniquement si la fenêtre principale est ouverte. Le programme sera déchargé dès que la fenêtre principale sera fermée.

Le programme Bart PE, installé par défaut, ne prend pas en charge les fichiers chm et le navigateur Internet. Cela signifie que l'aide de Kaspersky Internet Security et les conseils dans l'interface du logiciel ne sont pas accessibles en mode de restauration.

16.10. Utilisation des services complémentaires

Kaspersky Internet Security vous propose également les services complémentaires suivants :

- Avertissement de l'utilisateur par courrier électronique en cas d'événements particuliers.
- Autodéfense de Kaspersky Internet Security contre la désactivation, la suppression ou la modification des modules et protection de l'accès au logiciel par mot de passe.
- Economie de la charge de la batterie lors de l'utilisation du logiciel sur un ordinateur portable.

16.10.1. Notifications relatives aux événements de Kaspersky Internet Security

Différents types d'événements peuvent survenir pendant le fonctionnement de Kaspersky Internet Security. Ces notifications peuvent avoir un caractère purement informatif ou présenter des informations plus importantes. Par

exemple, la notification peut signaler la réussite de la mise à jour ou signaler une erreur dans le fonctionnement d'un composant qu'il faudra rectifier au plus vite.

Afin d'être au courant de ce qui se passe dans le cadre du fonctionnement de Kaspersky Internet Security, vous pouvez activer le service de notification. Ce service est prévu pour vous avertir des événements qui surviennent.

La notification peut être réalisée de l'une des manières suivantes :

- Infobulles au-dessus de l'icône du logiciel dans la barre des tâches.
- Notification sonore.
- Messages électroniques.

Pour utiliser ce service :

1. Cochez la case **Activer les notifications des événements** dans le bloc **Interaction avec l'utilisateur**(cf. ill. 98).

Illustration 98. Activation des notifications

2. Définir le type d'événements de Kaspersky Internet Security au sujet desquels vous souhaitez être averti, ainsi que le mode de notification (cf. point 16.10.1.1, p. 267).
3. Configurez les paramètres d'envoi des notifications par courrier électronique si vous avez choisi ce mode (cf. point 16.10.1.2, p. 269).

16.10.1.1. Types de notification et mode d'envoi des notifications

Différents types d'événements peuvent survenir pendant le fonctionnement de Kaspersky Internet Security.

Evénements critiques. Evénements critiques au sujet desquels il est vivement conseillé d'être averti car ils indiquent un problème dans le fonctionnement du logiciel ou une vulnérabilité dans la protection de l'ordinateur. Par exemple, *signatures des menaces corrompues* ou *expiration de la validité de la licence*.

Evénements importants. Evénements auxquels il faut absolument prêter attention car ils indiquent une situation importante dans le

fonctionnement du logiciel. Exemple : *protection désactivée* ou *l'analyse antivirus de l'ordinateur a été réalisée il y a longtemps*.

Evénements informatifs. Evénements à caractère purement informatif qui ne contient aucune information cruciale. Exemple : *tous les objets dangereux ont été réparés*.

Afin d'indiquer les événements au sujet desquels vous souhaitez être averti et de quelle manière :

1. Cliquez sur le lien Configuration dans la fenêtre principale du logiciel.
2. Dans la boîte de configuration du logiciel, sélectionnez la section **Service**, cochez la case ☑ **Activer les notifications sur les événements** et passez à la configuration détaillée en cliquant sur **Complémentaire**.

Sur l'onglet **Evénements** (cf. ill. 99) de la fenêtre qui s'ouvre, vous pouvez définir les modes d'envoi suivants pour les notifications :

- *Infobulles* au-dessus de l'icône du logiciel dans la barre des tâches contenant les informations relatives à l'événement ;

  Pour utiliser ce mode, cochez la case ☑ dans le schéma **Ecran** en regard de l'événement au sujet duquel vous souhaitez être averti.

- *Notification sonore.*

  Si vous voulez accompagner cette infobulle d'un effet sonore, cochez la case ☑ dans la partie **Son** en regard de l'événement.

- *Notification par courrier* électronique.

  Pour utiliser ce mode, cochez la case ☑ **Message** en regard de l'événement au sujet duquel vous souhaitez être averti et configurez les paramètres d'envoi des notifications (cf. point 16.10.1.2, p. 269).

Illustration 99. Evénement survenus pendant le fonctionnement du logiciel et modes de notification choisis.

16.10.1.2. Configuration de l'envoi des notifications par courrier électronique

Après avoir sélectionné les événements (cf. point 16.10.1.1, p. 267)au sujet desquels vous souhaitez être averti par courrier électronique, vous devez configurer l'envoi des notifications. Pour ce faire :

1. Ouvrez la fenêtre des paramètres du logiciel en cliquant sur le lien Configuration dans la fenêtre principale.
2. Sélectionnez le point **Service** dans l'arborescence des paramètres.
3. Cliquez sur le bouton **Complémentaire** dans le bloc **Interaction avec l'utilisateur** de la partie droite de la fenêtre.
4. Sélectionnez les paramètres d'envoi des notifications dans l'onglet **Notifications** (cf. ill. 100):
    - Définissez les paramètres d'expédition de la notification dans le bloc **Envoi de la notification au nom de l'utilisateur**.
    - Saisissez l'adresse électronique vers laquelle la notification sera envoyée dans le bloc **Destinataire des notifications**.

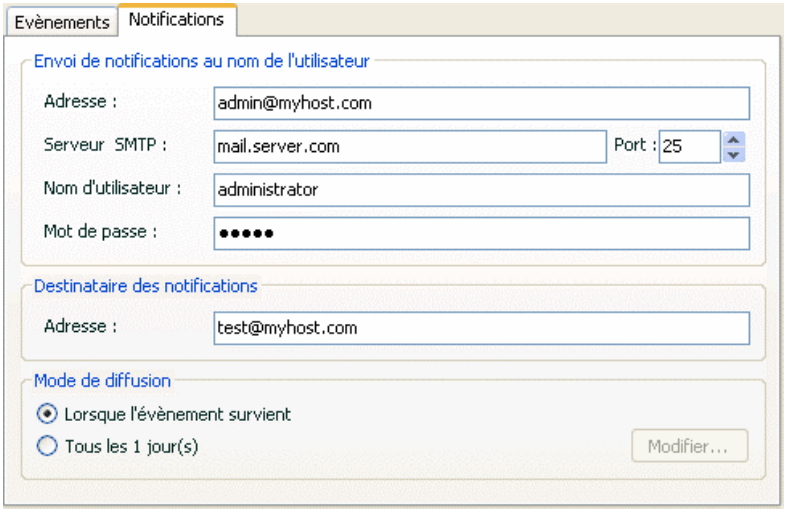


Illustration 100. Configuration de la notification par courrier électronique

- Définissez le mode d'envoi de la notification par courrier électronique dans le bloc **Mode de diffusion**. Afin que l'application envoie un message lorsqu'un événement se produit, sélectionnez **Lorsque l'événement survient**. Pour être averti des événements après un certain temps, programmez la diffusion des messages d'informations en cliquant sur le bouton **Modifier**. Par défaut, les notifications sont envoyées chaque jour.

16.10.2. Autodéfense du logiciel et restriction de l'accès

Kaspersky Internet Security est un logiciel qui protège les ordinateurs contre les programmes malveillants et qui pour cette raison constitue une cible de choix pour les programmes malveillants qui tentent de le bloquer ou de le supprimer de l'ordinateur.

De plus, un ordinateur personnel peut être utilisé par plusieurs personnes, qui ne possèdent pas toutes les mêmes connaissances en informatique. L'accès ouvert au logiciel et à ces paramètres peut considérablement réduire le niveau de la protection globale de l'ordinateur.

Afin de garantir la stabilité du système de protection de votre ordinateur, le logiciel incorpore un mécanisme d'autodéfense contre les interactions distantes ainsi que la protection de l'accès via un mot de passe.

Afin d'activer l'utilisation des mécanismes d'autodéfense du logiciel :

1. Ouvrez la fenêtre des paramètres du logiciel en cliquant sur le lien Configuration dans la fenêtre principale.
2. Sélectionnez le point **Service** dans l'arborescence des paramètres.
3. Opérez la configuration requise dans le bloc **Protection** (cf. ill. 101) :

   Activer l'autodéfense du programme. Lorsque cette case est cochée, le mécanisme de protection du programme contre la modification ou la suppression de ces propres fichiers sur le disque, des processus en mémoire et des enregistrement dans la base de registre système est activée.

   Interdire l'administration externe par un service. En cochant cette case, vous bloquez toute tentative d'administration à distance des services du programme

   Un message d'avertissement apparaîtra au-dessus de l'icône du programme dans la barre des tâches en cas de tentative d'exécution des actions citées.

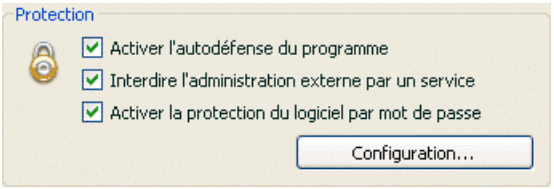


Illustration 101. Configuration de la protection du programme

Afin de limiter l'accès au logiciel à l'aide d'un mot de passe, cochez la case **Activer la protection du logiciel par mot de passe** et dans la fenêtre qui s'ouvre une fois que vous aurez cliqué sur Configuration, précisez le mot de passe et le secteur d'application de celui-ci (cf. ill. 102). Vous pouvez bloquer n'importe quelle action du programme, à l'exception des notifications en cas de découverte d'objets dangereux ou interdire l'une des actions suivantes :

- Modifier les paramètres de fonctionnement du logiciel.
- Arrêter Kaspersky Internet Security.
- Désactiver la protection de votre ordinateur ou la suspendre pour un certain temps.

Chacune de ces actions entraîne une réduction du niveau de protection de votre ordinateur , aussi vous devez faire confiance aux personnes à qui vous confiez ces tâches.

Désormais, chaque fois qu'un utilisateur de votre ordinateur tentera d'exécuter les actions que vous avez sélectionnées, il devra saisir le mot de passe.

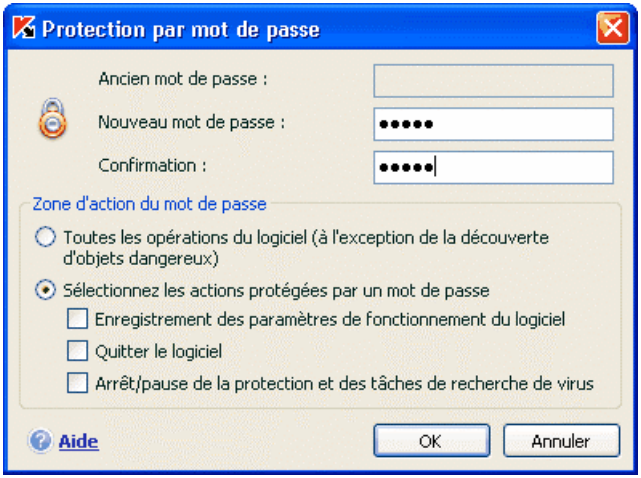


Illustration 102. Configuration de la protection par mot de passe

16.10.3. Configuration de la productivité

Afin d'économiser les batteries des ordinateurs portables et afin de limiter la charge appliquée au processeur central et aux sous-systèmes du disque, vous pouvez reporter les tâches liées à la recherche de virus.

- Etant donné que la recherche de virus et la mise à jour du logiciel sont assez gourmandes en ressources et durent un certain temps, nous vous conseillons de désactiver le lancement programmé de celles-ci. Cela vous permettra d'économiser la batterie. Au besoin, vous pourrez mettre à jour vous-même le programme (cf. point 5.8, p. 65) ou lancer l'analyse antivirus manuellement (cf. point 5.4, p. 62). Pour utiliser le service d'économie de la batterie, cochez la case correspondante dans la case **Alimentation et performances** (cf. ill. 103).

- L'exécution des tâches liées à la recherche de virus augmentent la charge du processeur central et des sous-systèmes du disque, ce qui ralentit le fonctionnement d'autres programmes. Lorsqu'une telle situation se présente, le programme arrête par défaut la recherche des virus et libère des ressources pour l'application de l'utilisateur.

Il existe cependant toute une série de programmes qui sont lancés lors de la libération des ressources du processeur et qui travaillent en arrière-plan. Afin que la recherche de virus ne dépendent pas du travail de tels programmes, cochez la case ☑ **Suspendre l'analyse si le processeur est occupé par d'autres applications**.

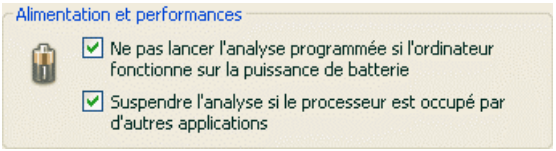


Illustration 103. Configuration de la productivité

CHAPITRE 17. UTILISATION DU PROGRAMME AU DEPART DE LA LIGNE DE COMMANDE

Vous pouvez utiliser Kaspersky Internet Security à l'aide de la ligne de commande. Ce mode vous permet d'exécuter les opérations suivantes :

- lancement, arrêt, suspension et reprise du fonctionnement des composants de l'application;
- lancement, arrêt, suspension et reprise de l'exécution des tâches liées à la recherche de virus;
- obtention d'informations relatives à l'état actuel des composants et aux tâches et à leur statistiques;
- Analyse des objets sélectionnés;
- Mise à jour des signatures des menaces et des modules du programme;
- Appel de l'aide relative à la syntaxe de la ligne de commande;
- Appel de l'aide relative à la syntaxe de la ligne de commande;

La syntaxe de la ligne de commande est la suivante :

avp.com <commande> [paramètres]

Où `<commande>` peut être remplacé par :

START	lancement du composant ou de la tâche
PAUSE	suspension du composant ou de la tâche
RESUME	reprise du fonctionnement du composant ou de la tâche
STOP	arrêt du composant ou de la tâche
STATUS	affichage de l'état actuel du composant ou de la tâche
STATISTICS	affichage des statistiques du composant ou de la tâche
HELP	aide sur la syntaxe de la commande ou la liste des commandes

	commandes.
SCAN	Analyse antivirus des objets
UPDATE	Lancement de la mise à jour du programme
EXIT	Quitter le logiciel (l'exécution de la commande est possible uniquement avec la saisie du mode passe défini via l'interface du programme)
IMPORT	importation des paramètres de protection de Kaspersky Internet Security
EXPORT	exportation des paramètres de protection de Kaspersky Internet Security

Chaque commande possède ses propres paramètres, propres à chaque composant de Kaspersky Internet Security.

17.1. Administration des composants de l'application et des tâches

L'administration des composants et des tâches de Kaspersky Internet Security au départ de la ligne de commande s'opère à l'aide des commandes suivantes :

- START
- PAUSE
- RESUME
- STOP
- STATUS
- STATISTICS

La tâche ou le composant auquel la commande sera appliquée est définie par son paramètre.

Les commandes STOP et PAUSE sont exécutées uniquement sous saisie du mot de passe de Kaspersky Internet Security, défini via l'interface du logiciel.

Syntaxe de la commande :

```
avp.com <commande> <profile|taskid>
avp.com STOP
        PAUSE <profile|taskid> /password=<mot de
passe>
```

<profile|taskid> est remplacé par l'une des valeurs suivantes :

RTP	Tous les composants de la protection
FM	Antivirus de fichiers
EM	Antivirus de courrier électronique
WM	Antivirus Internet
BM	Défense proactive
ASPY	Anti-Escroc
AH	Anti-Hacker
AS	Anti-Spam
UPDATER	Mise à jour
SCAN_OBJECTS	Tâche "Recherche de virus"
SCAN_MY_COMPUTER	Tâche "Mon poste de travail"
SCAN_CRITICAL_AREAS	Tâche "Secteurs critiques"
SCAN_STARTUP	Tâche "Objets de démarrage"
<nom_de_la_tâche>	Tâche créée par l'utilisateur

Les composants et les tâches lancés via la ligne de commande sont exécutés selon les paramètres définis dans l'interface du logiciel.

Exemples:

Par exemple, pour activer l'antivirus de fichiers via la ligne de commande, saisissez :

```
avp.com START FM
```

Afin d'afficher l'état actuel de la défense proactive de votre ordinateur, saisissez dans la ligne de commande:

```
avp.com STATUS BM
```

Pour arrêter la tâche Mon poste de travail via la ligne de commande, saisissez :

```
avp.com STOP SCAN_MY_COMPUTER
/password=<votre_mot_de_passe>
```

17.2. Analyse antivirus des fichiers

La ligne de commande utilisée pour lancer l'analyse antivirus d'un secteur quelconque et pour le traitement des objets malveillants découverts ressemble à ceci :

```
avp.com SCAN [<objet à analyser>] [<action>]
[<confirmation de l'action>] [<types de fichiers>]
[<exclusions>] [<fichier de configuration>]
[<paramètres du rapport>]
```

Pour analyser les objets, vous pouvez également utiliser les tâches créées dans Kaspersky Internet Security en lançant la tâche requise via la ligne de commande (cf. point 17.1, page 275). Dans ce cas, la tâche sera réalisée selon les paramètres définis dans l'interface du logiciel.

Description des paramètres.

<objet à analyser> ce paramètre définit la liste des objets qui seront soumis à la recherche de code malveillant.

Il peut contenir plusieurs des valeurs de la liste ci-après, séparées par un espace.

<files>	Liste des chemins d'accès aux fichiers et/ou aux répertoires à analyser. La saisie d'un chemin relatif ou absolu est autorisée. Les éléments de la liste doivent être séparés par un espace. Remarques : • Mettre le nom de l'objet entre guillemets s'il contient un espace; • Lorsqu'un répertoire particulier a été défini, l'analyse porte sur tous les fichiers qu'il contient.
/MEMORY	objets de la mémoire vive.
/STARTUP	objets de démarrage.
/MAIL	bases de données de messagerie électronique.
/REMDRIVES	tous les disques amovibles.
/FIXDRIVES	tous les disques locaux.
/NETDRIVES	tous les disques de réseau.
/QUARANTINE	objets en quarantaine.
/ALL	Analyse complète de l'ordinateur.
/@:<filelist.lst>	chemin d'accès au fichier de la liste des objets et répertoires inclus dans l'analyse. Le fichier doit être au format texte et chaque nouvel objet doit être mis à la ligne. La saisie d'un chemin relatif ou absolu est autorisée. Le chemin doit être saisi entre guillemets s'il contient un espace
<action> : ce paramètre définit les actions exécutées sur les objets malveillants découverts lors de l'analyse. Si le paramètre n'est pas défini, l'action exécutée par défaut sera l'action définie par la valeur **/i2.**	

/i0	aucune action n'est exécutée, seules les informations sont consignées dans le rapport..
/i1	réparer les objets infectés, si la réparation est impossible, les ignorer.
/i2	réparer les objets infectés, si la réparation est impossible, supprimer les objets simples; ne pas supprimer les objets infectés au sein d'un conteneur (fichiers composés); supprimer les conteneurs avec un en-tête exécutable (archive sfx) (cette action est exécutée par défaut).
/i3	réparer les objets infectés, si la réparation est impossible, supprimer complètement les conteneurs s'il n'est pas possible de supprimer les fichiers infectés qu'ils contiennent.
/i4	supprimer les objets infectés ; supprimer complètement les conteneurs s'il n'est pas possible de supprimer les fichiers infectés qu'ils contiennent.
Le paramètre **<confirmation de l'action>** définit les actions qui devront être confirmées par l'utilisateur lors de l'analyse. Si le paramètre n'est pas défini, l'action devra par défaut être confirmée à la fin de l'analyse.	
/a0	Ne pas confirmer l'action.
/a1	confirmer l'action lors de la découverte d'un objet infecté.
/a2	confirmer l'action à la fin de l'analyse
Le paramètre **<types de fichiers>** définit les types de fichiers qui seront soumis à l'analyse antivirus. Si le paramètre n'est pas défini, seuls seront analysés par défaut les objets pouvant être infectés en fonction du contenu.	
/fe	Analyser uniquement les fichiers qui peuvent être infectés selon l'extension.
/fi	Analyser uniquement les fichiers qui peuvent être infectés selon le contenu.

/fa	Analyser tous les fichiers.
Le paramètre **<exclusions>** définit les objets exclus de l'analyse. Il peut contenir plusieurs des valeurs de la liste ci-après, séparées par un espace.	
/e:a	Ne pas analyser les archives.
/e:b	Ne pas analyser les bases de messagerie.
/e:m	Ne pas analyser les messages électroniques au format plain text.
/e:<mask>	Ne pas analyser les objets en fonction d'un masque
/e:<seconds>	Ignorer les objets dont l'analyse dure plus que la valeur attribuée au paramètre <seconds>.
Le paramètre **<fichier de configuration>** définit le chemin d'accès au fichier de configuration qui contient les paramètres utilisés par le programme pour l'analyse. La saisie d'un chemin relatif ou absolu est autorisée. Si ce paramètre n'est pas défini, ce sont les valeurs définies dans l'interface de Kaspersky Internet Security qui seront utilisées.	
/C:<settings_file>	Utiliser les valeurs des paramètres définies dans le fichier **<settings_file>**.
Le paramètre **<paramètres du rapport>** définit le format du rapport sur les résultats de l'analyse. La saisie d'un chemin relatif ou absolu est autorisée. Si le paramètre n'est pas défini, les résultats de l'analyse seront affichés à l'écran et tous les événements seront repris.	
/R:<report_file>	Consigner uniquement les événements importants dans le fichier indiqué.
/RA:<report_file>	Consigner tous les événements dans le rapport.

Exemples:

*Lancer l'analyse de la mémoire vive, des objets de démarrage automatique, des bases de messagerie et des répertoires **My Documents, Program Files** et du fichier **test.exe**:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and
Settings\All Users\My Documents" "C:\Program Files"
"C:\Downloads\test.exe"
```

Suspendre l'analyse des objets sélectionnés, lancer une nouvelle analyse de l'ordinateur à la fin de laquelle il faudra poursuivre la recherche d'éventuels virus dans les objets sélectionnés :

```
avp.com PAUSE SCAN_OBJECTS
/password=<votre_mot_de_passe>
avp.com START SCAN_MY_COMPUTER
avp.com RESUME SCAN_OBJECTS
```

*Analyser les objets dont la liste est reprise dans le fichier **object2scan.txt.** Utiliser le fichier de configuration **scan_setting.txt**. A la fin de l'analyse, rédiger un rapport qui reprendra tous les événements.*

```
avp.com SCAN /MEMORY /@:objects2scan.txt
/C:scan_settings.txt /RA:scan.log
```

17.3. Mise à jour du logiciel

La commande de mise à jour des modules du logiciel et des signatures des menaces de Kaspersky Internet Security possède la syntaxe suivante :

```
avp.com UPDATE [<path/URL>] [/R[A]:<report_file>]
[/C:<settings_file>] [/APP]
```

Description des paramètres:

[<path/URL>]	Serveur HTTP, serveur FTP pou répertoire de réseau pour le chargement de la mise à jour. Si le chemin d'accès n'est pas indiquée, la source de la mise à jour sera définie par les paramètres du service de mise à jour de l'application.

/R[A]:<report_file>	**/R:<report_file>** : consigner uniquement les événements importants dans le rapport. **/R[A]:<report_file>** : consigner tous les événements dans le rapport. La saisie d'un chemin relatif ou absolu est autorisée. Si le paramètre n'est pas défini, les résultats de l'analyse seront affichés à l'écran et tous les événements seront repris.
/C:<settings_file>	Chemin d'accès au fichier de configuration contenant les paramètres de fonctionnement de l'application lors de la mise à jour. La saisie d'un chemin relatif ou absolu est autorisée. Si ce paramètre n'est pas défini, ce sont les valeurs définies dans l'interface de Kaspersky Internet Security qui seront utilisées.
/APP	Mettre a jour les modules du logiciel

Exemples:

Mettre à jour les signatures de menaces, consigner tous les événements dans le rapport :

```
avp.com UPDATE /RA:avbases_upd.txt
```

*Mettre à jour les modules de Kaspersky Internet Security en utilisant les paramètres du fichier de configuration **updateapp.ini**:*

```
avp.com UPDATE /APP /C:updateapp.ini
```

17.4. Exportation des paramètres

Syntaxe de la commande :

```
avp.com EXPORT <profile|taskid> <settings_file>
```

Description des paramètres:

<profile>	Composant ou tâche dont les paramètres sont exportés. Une des valeurs suivantes peut être utilisées : **RTP** = tous les composants de la protection. **FM** : Antivirus de fichiers. **EM** : antivirus de courrier électronique. **WM** : antivirus Internet. **BM** : défense proactive. **ASPY** : Anti-Escroc **AH** : Anti-Hacker. **AS** : Anti-Spam
<settings_file>	Chemin d'accès au fichier vers lequel sont exportés les paramètres de Kaspersky Internet Security. Vous pouvez indiquer un chemin relatif ou absolu. Seule l'utilisation de fichiers binaires (*cfg*.) est autorisée.

Exemples:

```
avp.com EXPORT c:\kis60settings.cfg
```

17.5. Importation des paramètres

Syntaxe de la commande :

```
avp.com IMPORT <settings_file>
```

<settings_file>	Chemin d'accès au fichier duquel sont importés les paramètres de Kaspersky Internet Security. Vous pouvez indiquer un chemin relatif ou absolu. Seule l'utilisation de fichiers binaires (*cfg*.) est autorisée.

Exemples:

```
avp.com IMPORT c:\kis60settings.cfg
```

17.6. Consultation de l'aide

Pour consulter l'aide au départ de la ligne de commande, utilisez la syntaxe suivante :

```
avp.com [ /? | HELP ]
```

Pour obtenir de l'aide sur la syntaxe d'une command particulière, vous pouvez utiliser une des commandes suivantes :

```
avp.com <commande> /?
avp.com HELP <commande>
```

CHAPITRE 18. MODIFICATION, REPARATION OU SUPPRESSION DU LOGICIEL

La réparation du logiciel est utile si vous êtes confrontés à certaines erreurs de fonctionnement suite à une mauvaise configuration ou à la corruption des fichiers de l'application.

La modification de la composition vous permet d'installer les composants manquants de Kaspersky Internet Security ou de supprimer ceux qui gênent votre travail ou qui sont inutiles.

Pour passer à la restauration de l'état d'origine du logiciel ou à l'installation de composants de Kaspersky Internet Security qui n'avaient pas été installés à l'origine ainsi que pour supprimer l'application :

1. Déchargez le programme de la mémoire système. Pour ce faire, cliquez avec le bouton droit de la souris sur l'icône du programme dans la barre des tâches et sélectionnez le point **Quitter** dans le menu contextuel.
2. Introduisez le cédérom d'installation dans le lecteur pour autant que vous ayez installé le logiciel à l'aide de ce cédérom. Si vous aviez procédé à l'installation au départ d'une autre source (dossier partagé, répertoire du disque dur, etc.), assurez que le fichier d'installation se trouve toujours dans le répertoire et que vous y avez accès.
3. Sélectionnez **Démarrez → Programmes → Kaspersky Internet Security 6.0 → Modification, réparation ou suppression**.

Cette action entraîne le lancement du programme d'installation qui se présente sous la forme d'un Assistant. Examinons les étapes de la réparation ou de la modification de la composition du logiciel ou de sa suppression.

Etape 1. Fenêtre d'accueil du programme d'installation

Si vous avez réalisé toutes les tâches nécessaires à la réparation ou à la modification de la composition du programme, la fenêtre d'accueil du programme d'installation de Kaspersky Internet Security s'affichera. Cliquez sur **Suivant** pour poursuivre.

Etape 2. Sélection de l'opération

Vous devez définir à cette étape le type d'opération que vous souhaitez exécuter sur le logiciel: vous pouvez soit modifier la composition du logiciel, soit restaurer l'état d'origine des composants installés ou supprimer certains composants ou l'application complète. Pour exécuter l'action que vous voulez, il suffit de cliquer sur le bouton correspondant. La suite de l'Assistant dépend de l'action que vous avez choisie.

La modification de la composition de l'application est similaire à l'installation personnalisée (cf. point Etape 6, p. 34) qui vous permet de sélectionner les composants que vous voulez installer ou supprimer.

La réparation du programme s'opère sur la base de la composition actuelle. Tous les fichiers des composants installés seront actualisés et pour chacun d'entre eux, c'est le niveau de protection Recommandé qui sera appliqué.

Lors de la suppression du logiciel, vous devrez sélectionner les données créées et utilisées par le programme que vous souhaitez sauvegarder. Pour supprimer toutes les données de Kaspersky Internet Security, sélectionnez l'option **Supprimer l'application complète**. Pour sauvegarder les données, vous devrez sélectionner l'option **Enregistrer les objets de l'application** et précisez quels objets exactement :

- *Informations relatives à l'activation* : clé de licence ou code d'activation du programme.
- *Signatures des menaces* : toutes les signatures des programmes dangereux, des virus et des autres menaces qui datent de la dernière mise à jour.
- *Base des connaissances d'Anti-Spam* : base de données qui contribue à l'identification du courrier indésirable. Cette base contient des informations détaillées sur les messages qui, pour vous, sont considérés comme des messages non sollicités ou des messages utiles.
- *Objets du dossier de sauvegarde* : copies de sauvegarde des objets supprimés ou réparés. Il est conseillé de sauvegarder ces objets en vue d'une restauration ultérieure.
- *Objets de la quarantaine* : objets qui sont peut-être modifiés par des virus ou leur modification. Ces objets contiennent un code semblable au code d'un virus connu mais qui ne peuvent être classés catégoriquement comme un virus. Il est conseillé de les conserver car ils ne sont peut-être pas infectés ou il sera possible de les réparer après la mise à jour des signatures des menaces.
- *Paramètres de la protection* : valeurs des paramètres de fonctionnement de tous les composants du logiciel.

- *Données iSwift* : base contenant les informations relatives aux objets analysés dans le système de fichiers NTFS. Elle permet d'accélérer l'analyse des objets. Grâce à cette base, Kaspersky Internet Security analyse uniquement les objets qui ont été modifiés depuis la dernière analyse.

> Attention.
>
> Si un laps de temps important s'écoule entre la suppression d'une version de Kaspersky Internet Security et l'installation d'une autre, il n'est pas conseillé d'utiliser la base iSwift de l'installation précédente. En effet, pendant cet intervalle, un programme dangereux peut s'infiltrer et ses actions pourraient ne pas être identifiées à l'aide de cette base, ce qui entraînerait l'infection de l'ordinateur.

Pour exécuter l'action sélectionnée, cliquez sur **Suivant**. La copie des fichiers nécessaires ou la suppression des composants et des données sélectionnés est lancée.

Etape 3. Liste des programmes pouvant nuire à la réparation, à la modification ou à la suppression du logiciel

S'il s'avère que les fichiers du logiciel sont utilisés par d'autres applications durant la réparation, la modification ou la suppression, la liste reprenant leur nom apparaîtra. En règle générale, cette liste contient les applications qui contiennent des plug in de Kaspersky Internet Security. Vous devrez les quitter.

Si vous souhaitez poursuivre l'opération en ignorant le conseil, cliquez sur **Ignorer**. Pour poursuivre l'exécution de l'opération une fois que vous aurez quitté les applications citées, cliquez sur le bouton **Réessayer**.

Etape 4. Fin de la réparation, de la modification ou de la suppression du logiciel

La progression de la réparation, de la modification ou de la suppression sera illustrée et vous serez averti dès que l'opération sera terminée.

En règle générale, la suppression requiert le redémarrage de l'ordinateur, indispensable pour tenir compte des modifications dans le système. La boîte de dialogue vous invitant à redémarrer l'ordinateur s'affichera. Cliquez sur **Oui** pour redémarrer immédiatement. Si vous souhaitez redémarrer l'ordinateur manuellement plus tard, cliquez sur **Non**.

CHAPITRE 19. QUESTIONS FRÉQUEMMENT POSÉES

Ce chapitre est consacré aux questions les plus fréquentes des utilisateurs sur l'installation, la configuration et l'utilisation de Kaspersky Internet Security. Nous avons tenté d'y répondre de la manière la plus exhaustive qui soit.

Question : Kaspersky Internet Security 6.0 peut-il être utilisé simultanément avec les logiciels d'autres éditeurs ?

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

Question : Kaspersky Internet Security n'analyse pas le fichier une deuxième fois. Pourquoi ?

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

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

Question : a quoi sert la clé de licence? Kaspersky Internet Security fonctionnera-t-il sans elle ?

Kaspersky Internet Security peut fonctionner sans clé de licence, mais dans ce cas la mise à jour de l'application et le service d'assistance technique seront inaccessibles.

Si vous n'avez pas encore pris la décision d'acheter Kaspersky Internet Security, nous pouvons vous transmettre une clé d'évaluation qui sera valide deux semaines ou un mois. Une fois la durée de validité écoulée, la clé sera bloquée.

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

Une telle situation est rare mais peut se produire en cas d'incompatibilité entre Kaspersky Internet Security et un autre programme installé sur votre ordinateur.

Pour rétablir le bon fonctionnement de votre système d'exploitation, suivez ces instructions :

1. Appuyez sur **F8** au tout début du démarrage de l'ordinateur jusqu'à ce que le menu de sélection du mode de démarrage apparaisse.
2. Sélectionnez le point **Mode sans échec** et chargez le système d'exploitation.
3. Lancez Kaspersky Internet Security.
4. Dans la fenêtre principale du logiciel, cliquez sur Configuration et sélectionnez la section **Protection** dans la boîte de dialogue de configuration.
5. Désélectionnez la case **Exécuter Kaspersky Internet Security 6.0 au démarrage du système** et cliquez sur **OK**.
6. Redémarrer le système d'exploitation en mode normal.

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

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

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

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

ANNEXE A. AIDE

Cette annexe contient des informations sur le format des fichiers analysés, sur les masques autorisés et sur l'utilisation de ceux-ci lors de la configuration de Kaspersky Internet Security.

A.1. Liste des objets analysés en fonction de l'extension

Si vous avez coché la case **Analyser les programmes et les documents (selon l'extension),** Antivirus Fichiers réalisera une analyse minutieuse des fichiers portant l'extension suivante. Ces fichiers seront également analysés par l'Antivirus Courrier si ils sont repris dans le filtrages des objets joints :

com : fichier exécutable d'un logiciel dont la taille ne dépasse pas 64Ko.

exe : fichier exécutable, archive autoextractible.

sys : fichier système.

prg : texte du programme dBase, Clipper ou Microsoft Visual FoxPro, programme de la suite WAVmaker.

bin : fichier binaire.

bat : fichier de paquet.

cmd : fichier de commande Microsoft Windows NT (semblable au fichier bat pour DOS), OS/2.

dpl : bibliothèque Borland Delphi compactée.

dll : bibliothèque dynamique.

scr : fichier d'économiseur d'écran de Microsoft Windows.

cpl : module du panneau de configuration de Microsoft Windows.

ocx : objet Microsoft OLE (Object Linking and Embedding).

tsp : programme qui fonctionne en mode de partage du temps.

drv : pilote d'un périphérique quelconque.

vxd : pilote d'un périphérique virtuel Microsoft Windows.

pif : fichier contenant des informations sur un logiciel.

lnk : fichier lien dans Microsoft Windows.

reg : fichier d'enregistrement des clés de la base de registres système de Microsoft Windows.

ini : fichier d'initialisation.

cla : classe Java.

vbs : script Visual Basic.

vbe : extension vidéo BIOS.

js, jse : texte source JavaScript.

htm : document hypertexte.

htt : préparation hypertexte de Microsoft Windows.

hta : fichier hypertexte utilisé pour la mise à niveau de la base de registres système du système d'exploitation.

asp : script Active Server Pages.

chm : fichier HTML compilé

pht : fichier HTML avec scripts PHP intégrés.

php : script intégré dans les fichiers HTML.

wsh : fichier de configuration de Windows Script Host.

wsf : script Microsoft Windows.

hlp : fichier d'aide au format Win Help.

eml : message électronique de Microsoft Outlook Express.

nws : nouveau message électronique de Microsoft Outlook Express.

msg : message électronique de Microsoft Mail.

plg : message électronique

mbx : extension des messages Microsoft Office Outlook sauvegardés.

doc : document Microsoft Office Word.

dot : modèle de document Microsoft Office Word.

fpm : programme de bases de données, fichier de départ de Microsoft Visual FoxPro.

rtf : document au format Rich Text Format.

shs : fragment de Shell Scrap Object Handler.

dwg : base de données de dessins AutoCAD.

msi : paquet Microsoft Windows Installer.

otm : projet VBA pour Microsoft Office Outlook.

pdf : document Adobe Acrobat.

swf : objet d'un paquet Shockwave Flash.

jpg, jpeg : fichier graphique de conservation de données compressées.

emf : fichier au format Enhanced Metafile. Nouvelle génération de métafichiers du système d'exploitation Microsoft Windows. Les fichiers EMS ne sont pas pris en charge par Microsoft Windows 16 bit.

ico : fichier d'icône de certains programmes (Microsoft Windows, Unix, Gimp).

ov? : fichiers exécutable MS DOC

*xl** : documents et fichiers de Microsoft Office Excel tels que : *xla*, extension Microsoft Excel ; *xlc* , schéma ; *xlt* , modèle de document, etc..

*pp** : documents et fichiers de Microsoft Office PowerPoint tels que : *pps* , dia Microsoft Office PowerPoint ; *ppt* , présentation, etc.

*md** : documents et fichiers de Microsoft Office Access tels que : *mda* , groupe de travail de Microsoft Office Access ; mdb, base de données, etc.

N'oubliez pas que le format du fichier peut ne pas correspondre au format indiqué par l'extension du fichier.

A.2. Masques autorisés pour l'exclusion de fichiers

Voici des exemples de masques que vous utilisez lors de la constitution de la liste d'exclusions des fichiers :

1. Masques sans chemin vers les fichiers :
   - ***.exe** : tous les fichiers **.exe*
   - ***.exe?** tous les fichiers **.ex?* où " ? " représente n'importe quel caractère
   - **test** : tous les fichiers portant le nom *test*
2. Masque avec chemin d'accès absolu aux fichiers :
   - **C:\dir*.*** ou **C:\dir* C:\dir** : tous les fichiers du répertoire *C:\dir*
   - **C:\dir*.exe** : tous les fichiers **.exe* du répertoire *C:\dir*
   - **C:\dir*.ex?** tous les fichiers *.ex? du répertoire *C:\dir* où " ? " représente n'importe quel caractère unique
   - **C:\dir\test** : uniquement le fichier *C:\dir\test*

   Afin que les fichiers ne soient pas analysés dans tous les sous-répertoires du répertoire indiqué, cochez la case **Sous-répertoires compris**.
3. Masque avec chemin d'accès relatifs aux fichiers :
   - **dir*.*** ou **dir*** ou **dir** : tous les fichiers dans tous les répertoires *dir*
   - **dir\test** : tous les fichiers *test* dans les répertoires *dir*

- **dir*.exe** : tous les fichiers **.exe* dans tous les répertoires *dir*\
- **dir*.ex?** tous les fichiers **.ex?* dans tous les répertoires *dir*\ où " ? " peut représenter n'importe quel caractère unique

Afin que les fichiers ne soient pas analysés dans tous les sous-répertoires du répertoire indiqué, cochez la case **Sous-répertoires compris**.

Conseil.

L'utilisation du masque ***.*** ou * est autorisée uniquement lorsque le verdict de la menace à exclure est indiqué. Dans ce cas, la menace indiquée ne sera pas identifiée dans les objets. L'utilisation de ces menaces sans indication du verdict revient à désactiver la protection en temps réel.

Il est également déconseillé de sélectionner parmi les exclusions le disque virtuel créé sur la base du répertoire du système de fichiers à l'aide de la commande *subst*. Cela n'a pas de sens car pendant l'analyse, le logiciel considère ce disque virtuel comme un répertoire et, par conséquente, l'analyse.

A.3. Masques d'exclusion autorisés en fonction du verdict

Pour ajouter des menaces d'un verdict particulier (conforme au classement de l'encyclopédie des virus) en guise d'exclusion, vous pouvez indiquer :

- le nom complet de la menace, tel que **repris** dans l'encyclopédie des virus sur http://www.viruslist.com/fr (ex. **not-a-virus:RiskWare.RemoteAdmin.RA.311** ou **Flooder.Win32.Fuxx**);
- Le nom de la menace selon un masque, par exemple :
  - **not-a-virus*** : exclut de l'analyse les logiciels licites mais potentiellement dangereux, ainsi que les jokewares.
  - ***Riskware.*** : exclut de l'analyse tous les types de logiciels présentant un risque potentiel de type Riskware.
  - ***RemoteAdmin.*** : exclut de l'analyse toutes les versions de logiciel d'administration à distance.

ANNEXE B. KASPERSKY LAB

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

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

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

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

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

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

B.1. Autres produits antivirus

Kaspersky Anti-Virus 6.0

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

Le programme assure une analyse antivirus sophistiquée, notamment :

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

La défense proactive permet de :

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

- **Restaurer le système** après les actions malveillantes des logiciels espion : grâce à la correction des modifications de la base de registres et du système de fichiers de l'ordinateur et leur remise à l'état antérieur sur décision de l'utilisateur.

Kaspersky Lab News Agent

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

News Agent permet également de:

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

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

Kaspersky OnLine Scanner

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

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

Kaspersky® OnLine Scanner Pro

Il s’agit d’un service payant offert aux visiteurs du site Internet de Kaspersky Lab et qui permet de réaliser une analyse antivirus efficace de l’ordinateur et de réparer les fichiers infectés en ligne. Kaspersky OnLine Scanner Pro fonctionne directement dans le navigateur à l’aide de la technologie Microsoft ActiveX®.

Ainsi, les utilisateurs peuvent obtenir de manière efficace des réponses à leurs inquiétudes sur une infection éventuelle. Dans le cadre de l'analyse, l'utilisateur peut :

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

Kaspersky® Security for PDA

Le logiciel Kaspersky® Security for PDA protège de manière fiable les données enregistrées sur vos appareils nomades de différents types et sur vos téléphones intelligents. Le logiciel contient un bouquet d'outils antivirus bien ciblés :

- **Un scanner antivirus** qui analyse, à la demande de l'utilisateur, les informations enregistrées aussi bien dans la mémoire du PDA ou du téléphone intelligent que sur n'importe quel type de carte mémoire ;
- **Un moniteur antivirus** qui intercepte les virus au cours de la synchronisation à l'aide de la technologie HotSync™ vers d'autres périphériques.

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

Kaspersky Anti-Virus® Business Optimal

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

Kaspersky Anti-Virus® Business Optimal offre une protection antivirale[3] intégrale de :

- Postes de travail sous Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstation et Linux ;
- *Serveurs de fichiers* sous Microsoft Windows NT 4.0 Server, Microsoft Windows 2000/2003 Server/Advanced Server, Novell Netware, FreeBSD et OpenBSD, Linux et Samba Servers ;
- *Système de messagerie* Microsoft Exchange 2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail et Qmail ;

[3] En fonction du type de livraison

- *Passerelle-Internet* : CheckPoint Firewall –1; Microsoft ISA Server 2000 Standard Edition.

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

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

Kaspersky® Corporate Suite

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

Kaspersky® Corporate Suite garantit la protection antivirale intégrale de :

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

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

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

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam est une suite logicielle performante conçue pour protéger les réseaux des petites et moyennes entreprises contre les courriers électroniques non désirés (spam). Ce produit combine les techniques révolutionnaires d'analyse linguistique des messages, avec l'ensemble des

méthodes de filtrage de courrier électronique modernes (y compris les listes noires, ou listes RBL). Il inclut une collection unique de services permettant aux utilisateurs d'identifier et de nettoyer près de 95% du trafic non souhaité.

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

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

Kaspersky SMTP Gateway

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

Kaspersky Security® for Microsoft Exchange 2003

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

Kaspersky® Mail Gateway

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

centralisé du courrier afin d'identifier le courrier indésirable. Le logiciel offre aussi plusieurs autres possibilités en matière de filtrage des flux de messagerie.

B.2. Coordonnées

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

Support technique	Pour une assistance technique, adressez-vous à : http://case.kaspersky.fr/
Informations générales	WWW : http://www.kaspersky.com/fr/ Virus : http://www.viruslist.com/fr/ Support : http://support.kaspersky.fr E-mail : info@fr.kaspersky.com

ANNEXE C. 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.

EN ACCORD AVEC LA LEGISLATION FRANCAISE, SI VOUS ETES UN PARTICULIER ET QUE VOUS AVEZ ACHETE VOTRE LOGICIEL EN FRANCE, VIA INTERNET, SUR UNE BOUTIQUE EN LIGNE, 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.

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.

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.

Le Logiciel est "en utilisation" sur un ordinateur lorsqu'il est chargé dans la mémoire tampon (i.e., random-access memory ou RAM) ou installé dans la mémoire permanente (e.g., disque dur, CD-ROM, ou autre périphérique de stockage) de 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.

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.

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

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.

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.

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.

Assistance technique.

Kaspersky peut vous fournir une assistance technique ("Assistance Technique") comme décrit sur le site www.kaspersky.fr.

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.

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

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 connus ou 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).

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; ou

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

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

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.