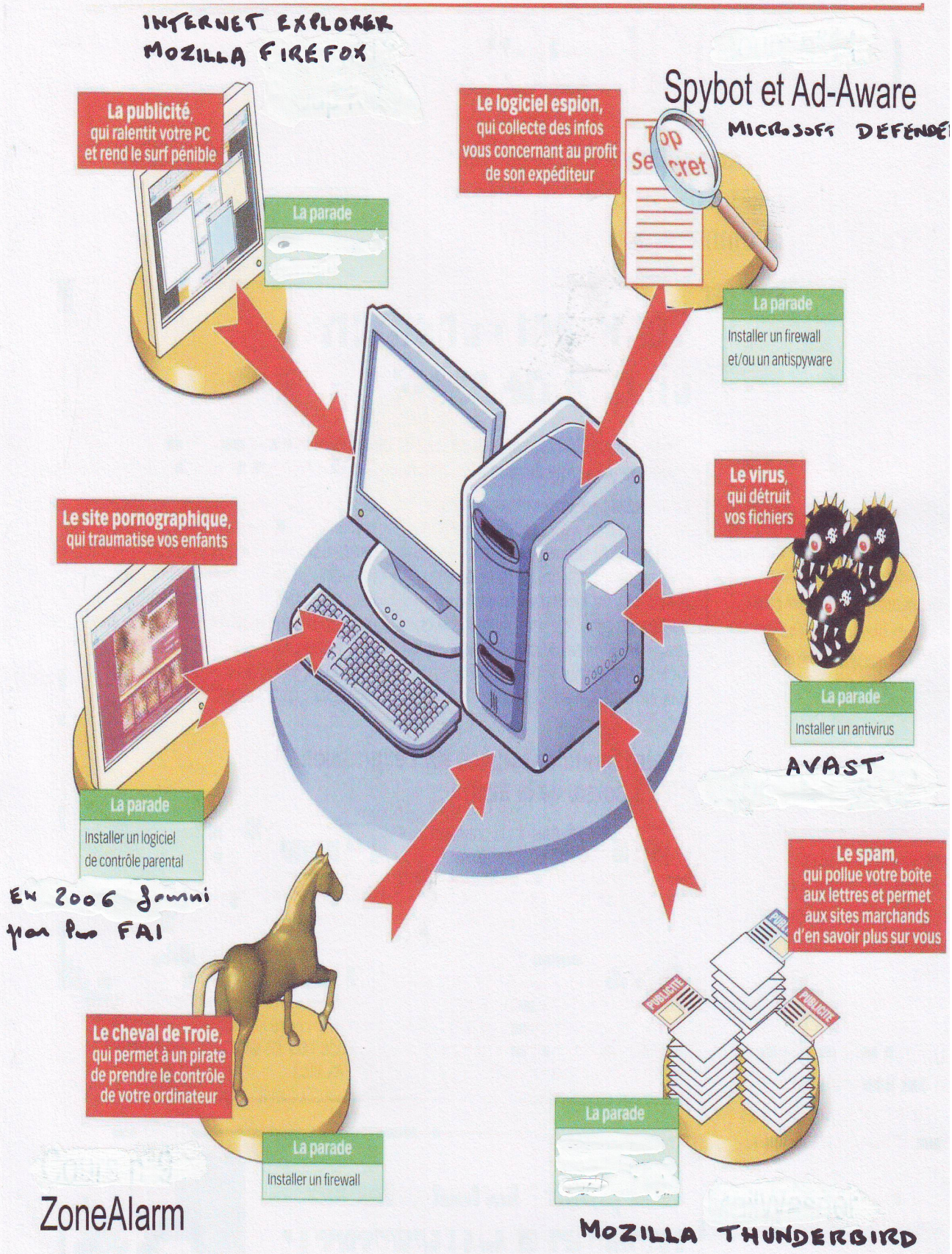
Protéger son PC gratuitement

Relié à Internet, un ordinateur devient la cible de multiples attaques, surtout lorsqu'il est connecté toute la journée en haut débit. Premier problème, les virus sont de plus en plus coriaces et malins. Il est loin, le temps où ils n'arrivaient que par disquettes ou par mails, en pièces jointes ! Aujourd'hui, la page Web d'apparence la plus anodine peut compromettre votre ordinateur lorsque vous l'affichez dans votre navigateur. Pire : une faille de sécurité dans Windows non corrigée peut permettre à un virus, tel Sasser il y a quelques mois, de s'installer sans aucune intervention de la part de l'utilisateur.

Autres dangers : les chevaux de Troie dont le rôle est de fournir une porte d'entrée sur votre PC à un pirate, ou encore les logiciels espions, glanant un maximum d'informations sur vos habitudes de navigation pour les revendre ensuite à des professionnels du marketing.

INTERNET EXPLORER
MOZILLA FIREFOX



Efficaces les logiciels gratuits ?

Pour surfer sans risque, il devient donc indispensable d'installer plusieurs logiciels de protection : un antivirus surveillant en permanence le système, un pare-feu contrôlant les données entrant et sortant du PC et un antiespion pour supprimer les programmes trop curieux. Mais si vous cherchez à vous procurer ces logiciels dans le commerce, la facture peut vite devenir salée : plus de 100 euros ! Si votre budget est serré, optez pour les logiciels gratuits. Sont-ils moins efficaces que les payants ? Pas toujours. Dans la pratique, la qualité de certains pare-feu et logiciels antiespions gratuits n'a rien à envier à leurs homologues payants. Vous pouvez donc vous équiper avec les programmes gratuits que nous proposons. Pour les antivirus, la principale différence entre les logiciels gratuits et payants réside dans les mises à jour. Nos tests l'ont démontré (voir *l'OI* n°160 page 86), là où les éditeurs de produits commerciaux mettent moins de 10 heures pour détecter de nouveaux virus, les développeurs des logiciels gratuits mettent jusqu'à 30 heures. Mais une fois mis à jour, les gratuits sont tout aussi efficaces. Enfin, quelle que soit la protection que vous adoptez, n'oubliez pas que votre comportement est déterminant pour votre sécurité. Entre les réglages de Windows, les sites que vous visitez et les programmes que vous téléchargez, vous devez toujours prendre garde à ce que vous faites.

Bien régler le système

Avant toute chose, commencez par limiter les risques liés à l'utilisation d'Internet en installant le Service Pack 2 de Windows XP et en paramétrant correctement votre système d'exploitation.

Installez la mise à jour du Service Pack 2

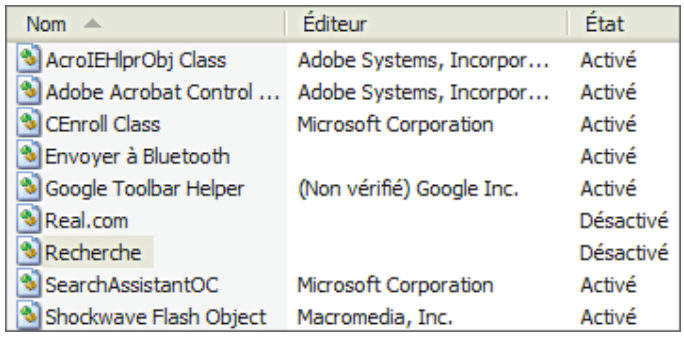
La dernière mise à jour de Windows XP apporte de nouvelles fonctions de protection : correctifs de failles de sécurité, pare-feu activé par défaut, centre de sécurité pour gérer la sécurité de l'ordinateur, contrôle précis des modules complémentaires d'Internet Explorer, et bien plus encore. Pour mettre à jour votre système, ouvrez Internet Explorer puis déroulez le menu **Outils, Windows Update.**

Le service de téléchargements de mises à jour de Microsoft pour Windows s'ouvre alors. Cliquez sur le lien **Installation rapide (recommandée).** Windows Update recherche alors les mises à jour disponibles pour votre ordinateur. Cliquez sur le bouton **Installer** puis acceptez le contrat de licence en cliquant sur **J'accepte.** Il vous suffit, ensuite, de suivre les étapes de l'installation, qui dure environ 20 minutes avec un accès à haut débit.

Paramétrez le système de protection anti-ActiveX

Après l'installation du SP2, un nouvel outil apparaît dans Internet Explorer, permettant de gérer les composants ActiveX. Ces programmes, aussi appelés modules complémentaires, sont utilisés par de nombreuses pages Web pour ajouter de nouvelles fonctions au navigateur Internet : affichage de vidéos, menus animés, etc. Mais ils peuvent aussi se révéler malveillants en installant des programmes à l'insu de l'utilisateur ou en changeant la page d'accueil.

Pour en contrôler le fonctionnement, paramétrez le gestionnaire de modules complémentaires d'Internet Explorer. Déroulez le menu **Outils, Gérer les modules complémentaires.** La liste des modules chargés dans Internet Explorer est alors affichée avec, pour chacun d'eux, le nom, l'éditeur et le type d'objet. Déroulez la liste **Afficher,** puis sélectionnez l'option **Modules complémentaires qui ont été utilisés par Internet Explorer.** Tous les modules, qu'ils soient actuellement exploités ou non, seront alors affichés.

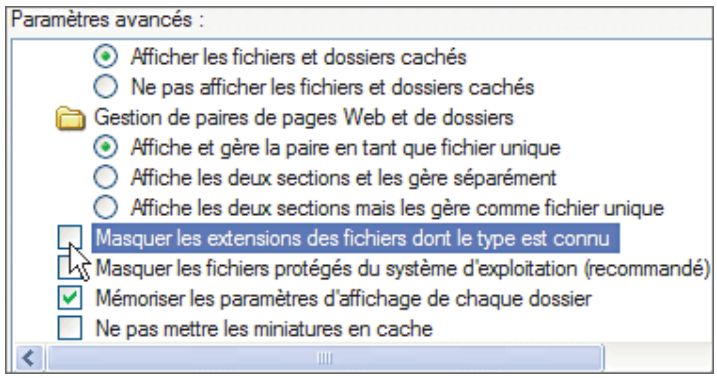


Identifiez ceux dont l'origine vous est inconnue, puis sélectionnez-les et cochez l'option **Désactiver** dans la zone **Paramètres.** Cliquez sur le bouton **OK** puis redémarrez Internet Explorer. Au besoin, si un site ne fonctionne plus correctement, vous pouvez activer un module précédemment désactivé en le sélectionnant puis en choisissant **Activer.**

Affichez les extensions de tous les types de fichiers

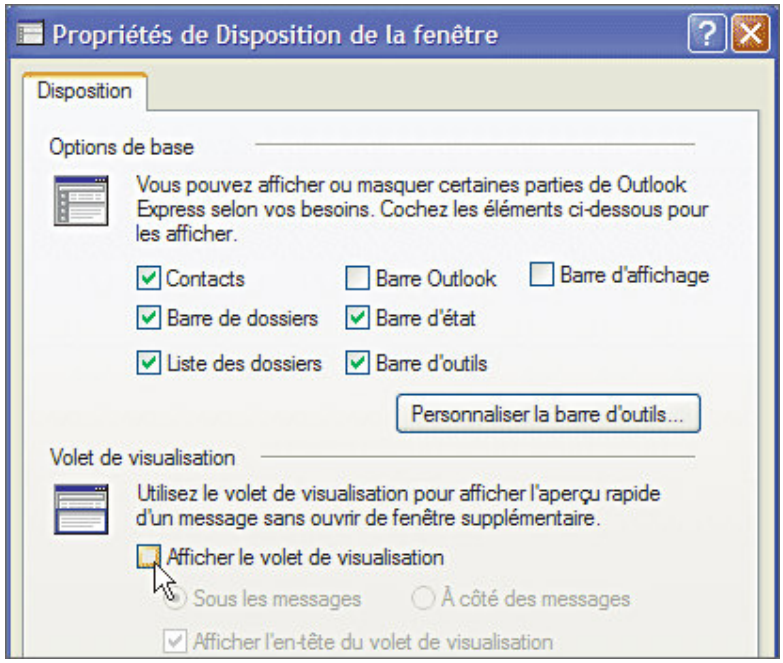
Par défaut, Windows XP masque les extensions de fichiers dont le type est connu (.doc pour Word, par exemple). Or, cela peut comporter des dangers, car certains scripts n'hésitent pas à maquiller leur extension pour vous inciter à les ouvrir. Ainsi, un fichier malicieux nommé **ski.jpg.exe** apparaîtra comme **ski.jpg** sous Windows, vous faisant croire que c'est une image au format JPeg alors qu'il s'agit d'un programme.

Pour éviter ce piège, vous devez afficher constamment toutes les extensions des fichiers. Pour cela, dans **l'Explorateur,** déroulez le menu **Outils, Options des dossiers.** Cliquez ensuite sur l'onglet **Affichage.** Dans la zone **Paramètres avancés,** décochez la case **Masquer les extensions des fichiers dont le type est connu.** Validez enfin par un clic sur **OK.**



Désactivez l'aperçu des mails dans Outlook Express

Certains virus contenus dans les courriels que vous recevez s'exécutent dès leur ouverture. Or par défaut, lorsque vous sélectionnez un mail, pour le supprimer par exemple, son contenu est affiché dans le volet de visualisation... et le message est ouvert. Il est donc préférable de ne plus afficher le contenu des mails. Pour cela, dans Outlook Express, déroulez **Affichage, Disposition.** Dans la rubrique **Volet de visualisation,** décochez la case **Afficher le volet de visualisation.** Validez enfin par **OK.**



Installer et configurer le pare-feu Kerio Personal Firewall

Limitez les tentatives des pirates pour prendre le contrôle de votre ordinateur en installant un logiciel qui filtre les échanges de données entre votre PC et Internet.

Chaque programme qui se connecte à Internet se voit attribuer une « adresse » unique : un port. Lorsque l'ordinateur reçoit des informations destinées à un port, les données sont envoyées vers le logiciel correspondant. Pour éviter que des programmes espions ou des chevaux de Troie ne transmettent des données sur Internet à votre insu, le plus simple est de bloquer tous les ports non utilisés par des logiciels connus. C'est le rôle du pare-feu, ou firewall.

Celui de Windows, appelé ICF, bloque ainsi par défaut tous les ports en réception de données (d'autres machines connectées à Internet ne peuvent pas envoyer des données vers votre PC) mais cette technique de filtrage ne vous protège pas totalement. En effet, ICF n'empêche pas un programme de votre ordinateur de diffuser des informations sur Internet, car tous les ports sont ouverts.

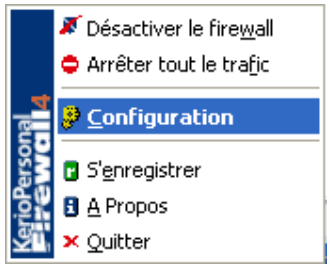
Il faut donc filtrer également les sorties, ce dont s'acquitte parfaitement Kerio Personal Firewall Fermant tous les ports de communication pour éviter les intrusions et vous demandant l'autorisation chaque fois qu'un programme tente de se connecter à Internet, il vous protège efficacement.

Kerio personnal firewall est un firewall en français. Il dispose d'une interface claire et simple à appréhender.

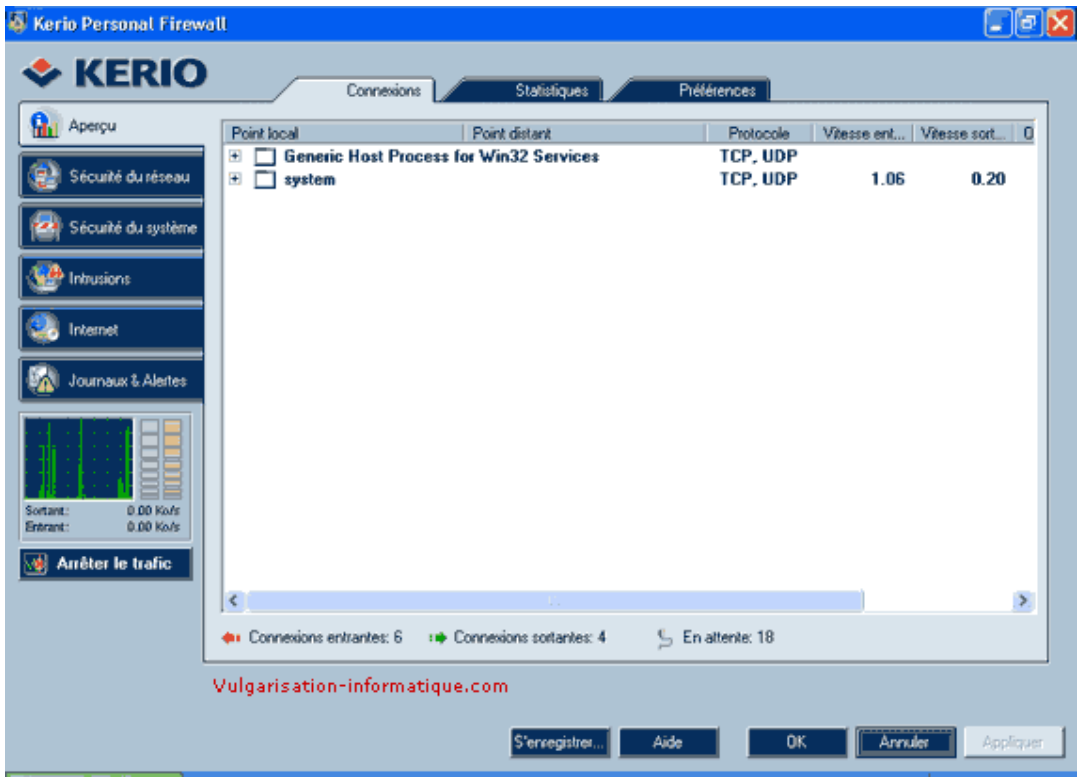
Vous pouvez commencer par télécharger kerio **ici**. Sélectionnez **anglais** pour la langue d'installation, et installez kerio. Redémarrez ensuite votre PC.

Une icône est ensuite visible dans le systray (à côté de l'horloge) :

Faites un clic droit sur cette icône, le menu permettant de configurer kerio s'affiche :



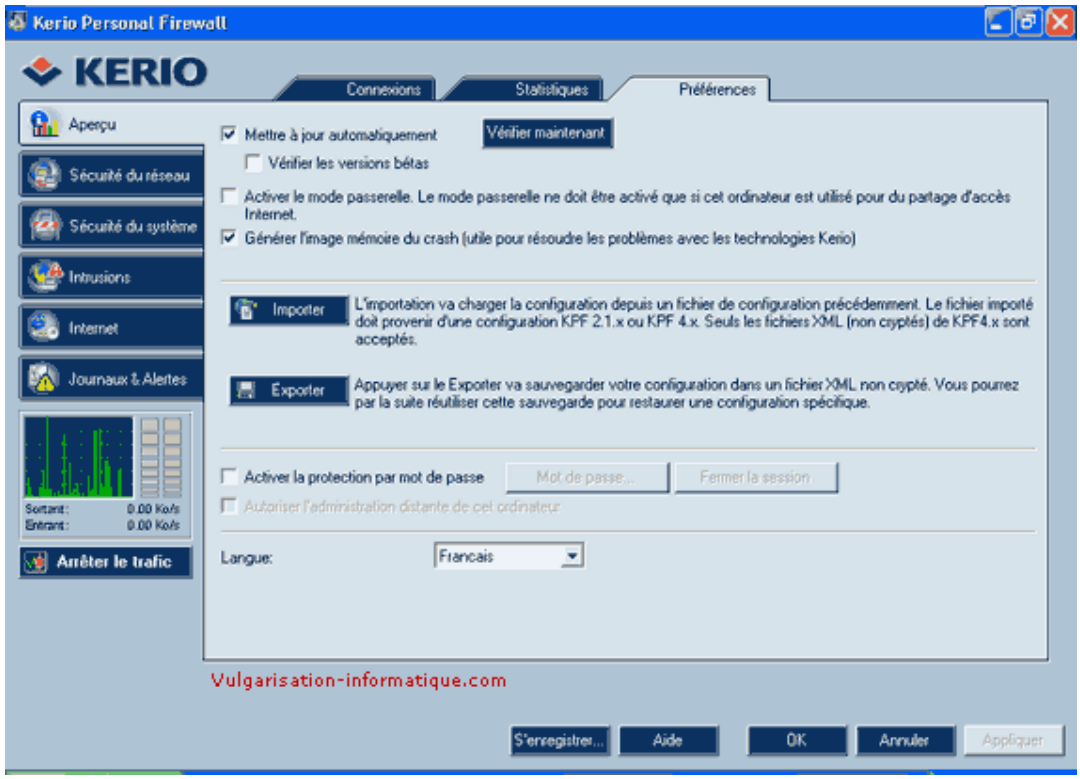
Cliquez sur **configuration**. Vous avez alors accès à toutes les options disponibles. L'écran d'accueil de kerio se présente sous cette forme :



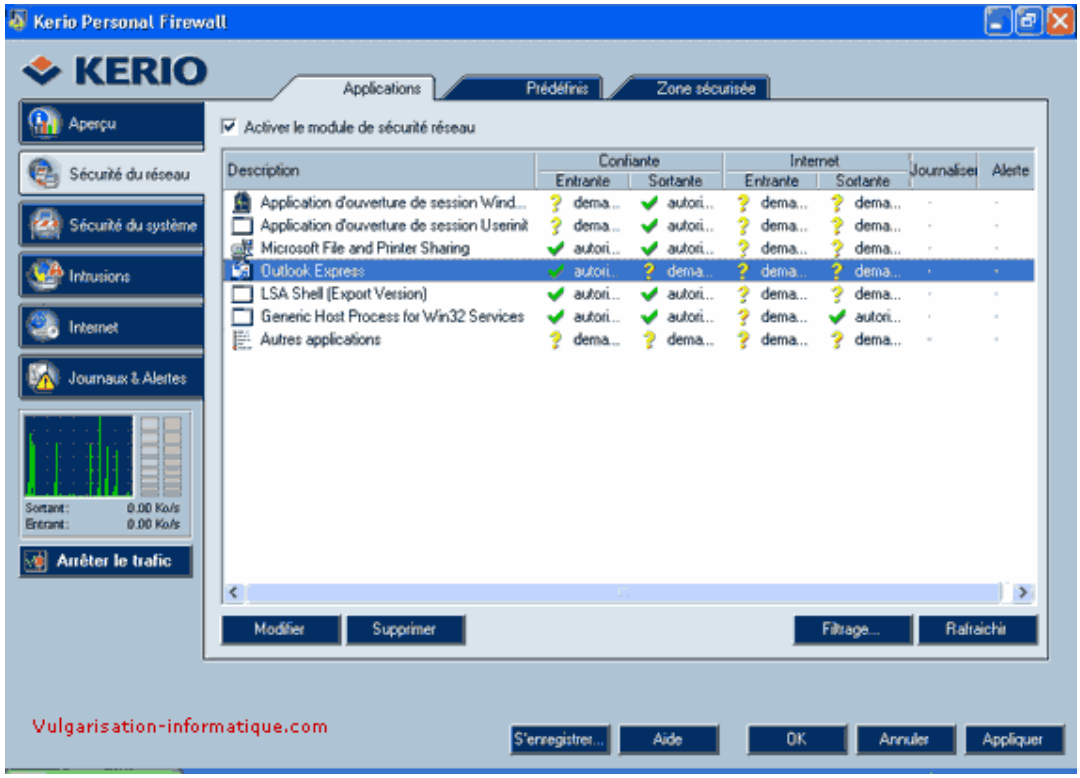
Cliquez sur un élément (ici **system**) pour afficher la liste des connexions entrantes et sortantes ainsi que les ports associés à ces connexions.

Cliquez sur l'onglet **statistiques**. Ici, en cliquant sur le groupe de statistiques que vous souhaitez consulter (par exemple **publicités**), toutes les actions modifiées ou bloquées par kerio s'afficheront sous forme de liste.

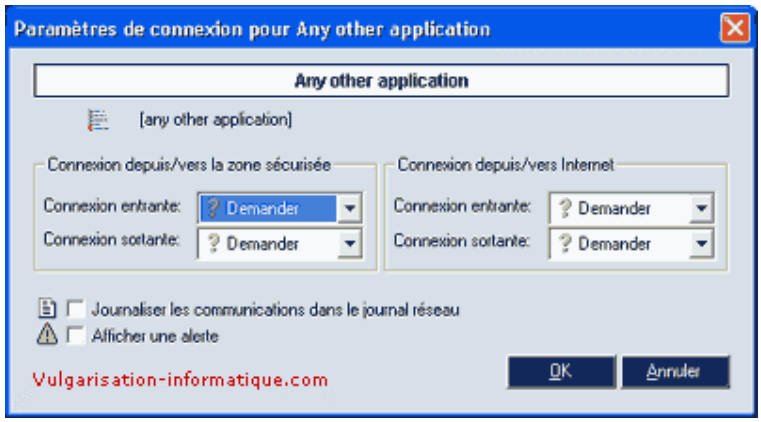
Cliquez ensuite sur l'onglet **préférences**. Vous pouvez ici configurer les options de base du logiciel. Cochez la case **Mettre à jour automatiquement** et décochez celle nommée **Vérifier les versions Beta**. Si vous souhaitez protéger la configuration de votre firewall, cochez la case **Activer la protection par mot de passe**.



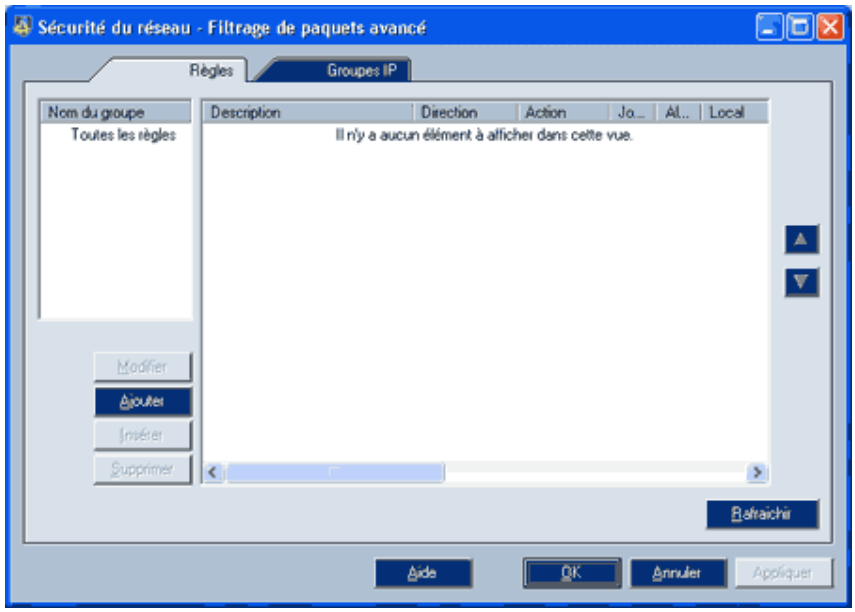
Cliquez ensuite sur **Sécurité du réseau**. Les choses un peu plus sérieuses commencent. Cochez tout d'abord la case **Activer le module de sécurité réseau**. Vous pouvez ici pour chaque application listée (ou toutes les autres en cliquant sur **autres applications**) refuser sa communication localement ou à travers internet.



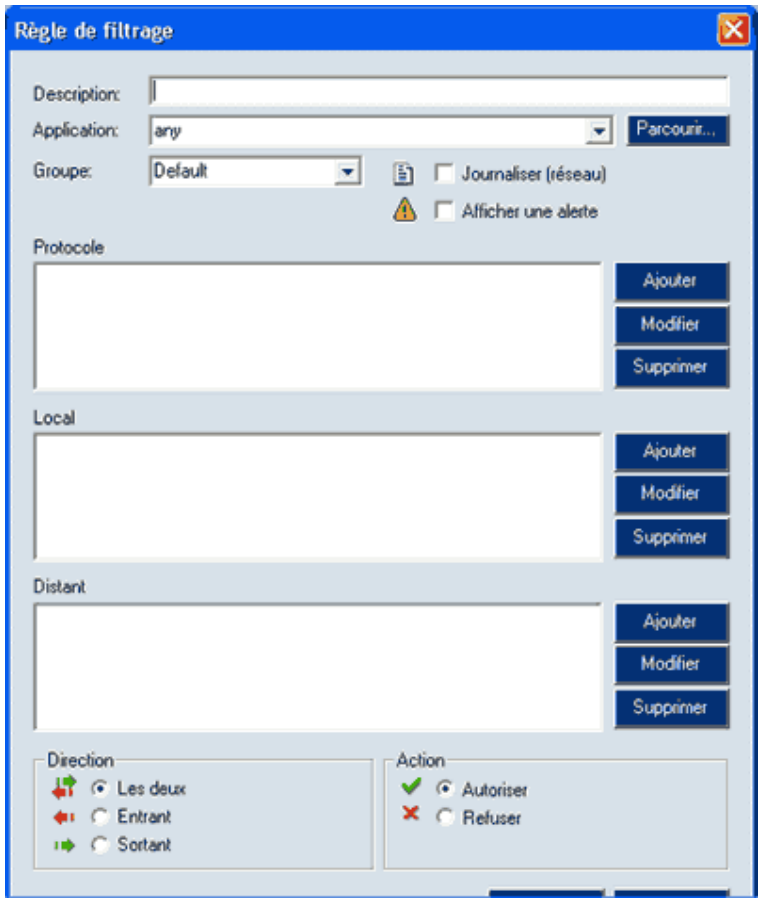
Pour modifier les droits de communication de l'application de votre choix, double cliquez sur sa description. Une fenêtre de ce type s'affiche :



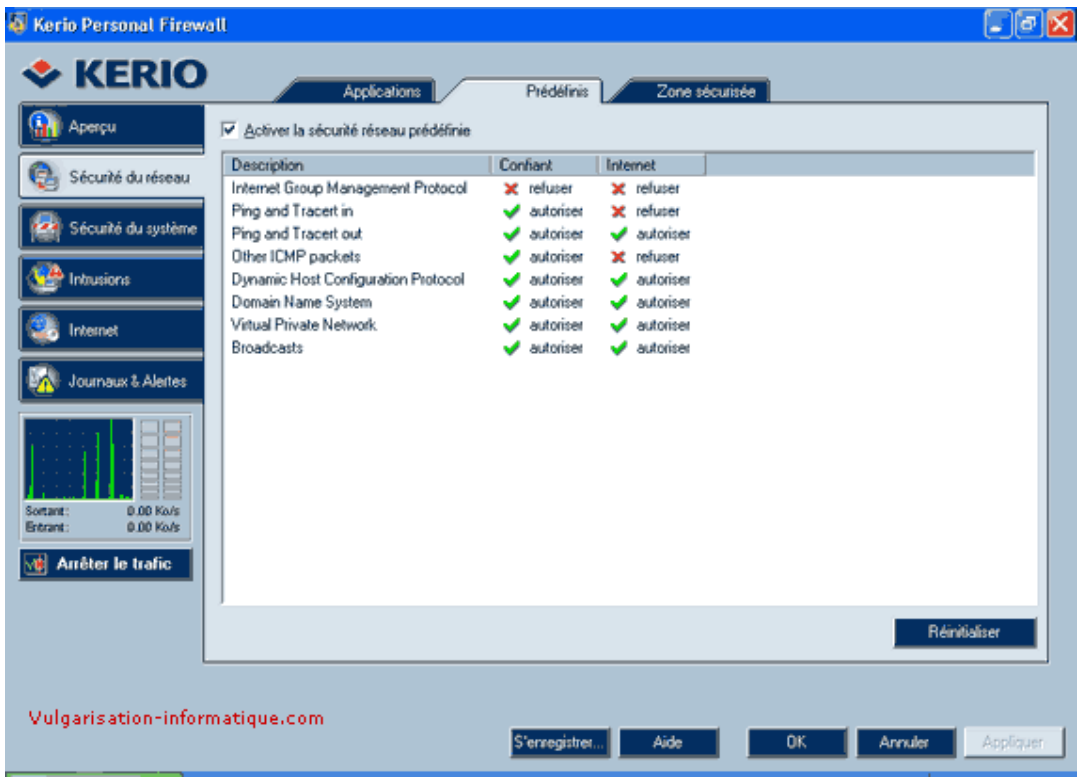
Modifiez les paramètres en fonction de la sécurité que vous souhaitez apporter. Pour un navigateur web, vous pouvez par exemple dans le cadre **Connexion depuis/vers la zone sécurisée** autoriser les connexions sortantes et refuser les connexions entrantes, de même pour internet. Une fois les paramètres modifiés cliquez sur **Ok**. Pour définir des règles de filtrage plus précises, cliquez ensuite sur le bouton **filtrage**. Les règles de filtrage s'affichent. Pour ajouter une règle de filtrage, cliquez sur **ajouter**.



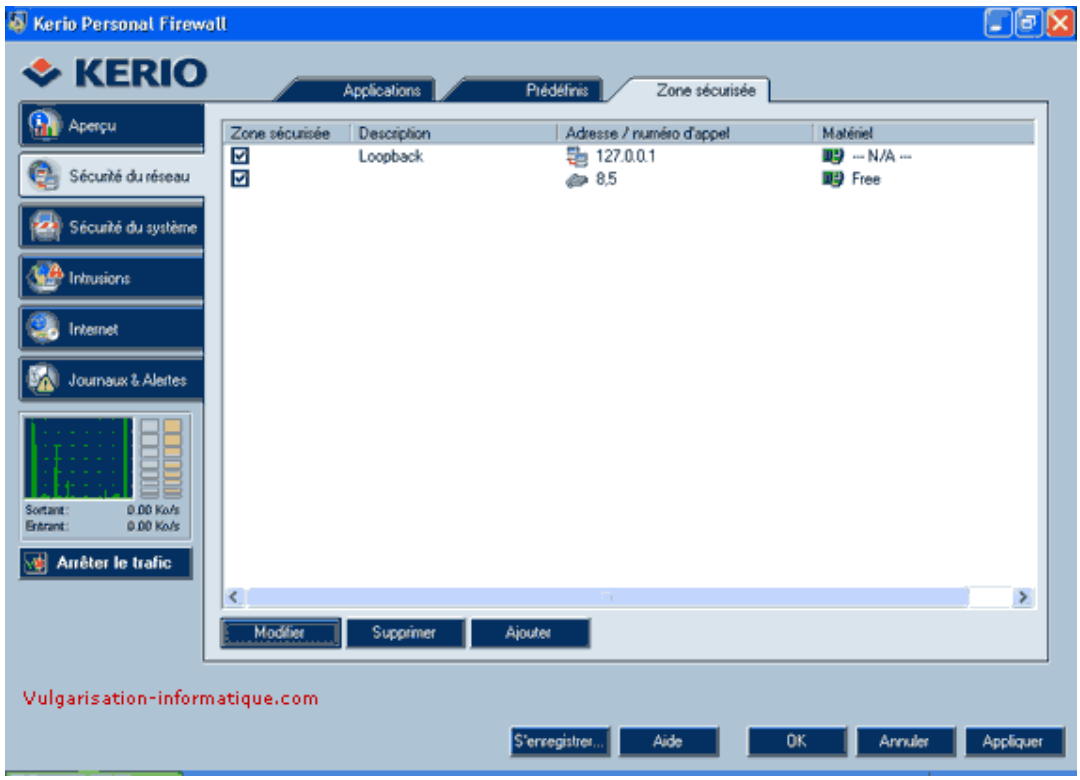
Une fenêtre de ce type s'affiche. Rentrez tout d'abord une description de la règle de filtrage, puis sélectionnez l'application pour laquelle elle doit s'appliquer. Si vous souhaitez que cette règle s'applique à toutes les applications, sélectionnez **Any**. Cliquez ensuite dans la zone **protocole** sur **ajouter** puis définissez le protocole pour lequel cette règle doit s'appliquer. Cliquez ensuite dans la zone **local** sur **ajouter** et ajoutez un port (80 par exemple pour le protocole HTTP) ou une plage de ports. Faites de même dans la zone **distant** (vous pouvez aussi ajouter une adresse ip ou une plage d'adresses ip).



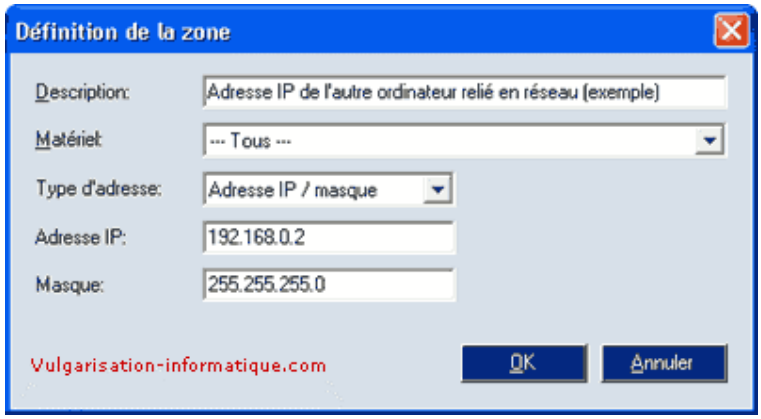
Sélectionnez ensuite la direction du trafic pour laquelle cette règle doit s'appliquer et ce qu'elle doit faire (refuser ou autoriser le trafic). Cliquez ensuite sur Ok. Cliquez ensuite sur l'onglet **prédéfinis** du menu **sécurité du réseau**. Vous pouvez ici refuser ou autoriser des commandes telles que **ping, tracert**...



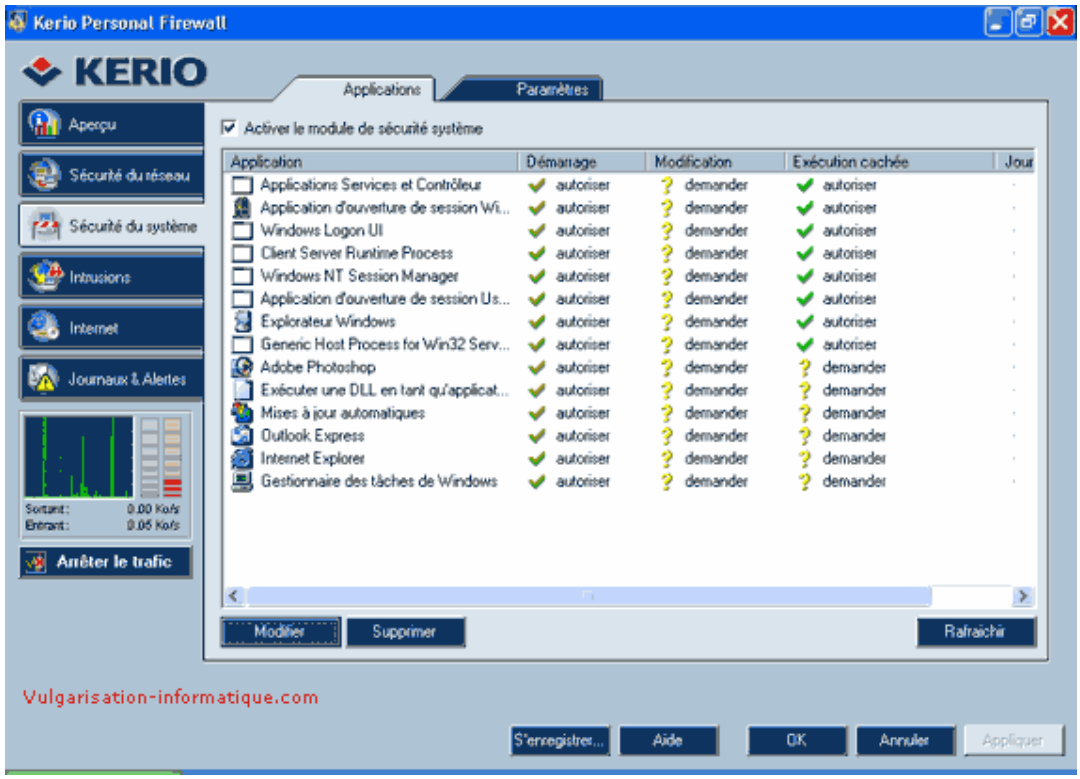
Cliquez ensuite sur l'onglet **zone sécurisée**. Vous pouvez donner ici des zones que Kerio considèrera comme étant sécurisées.



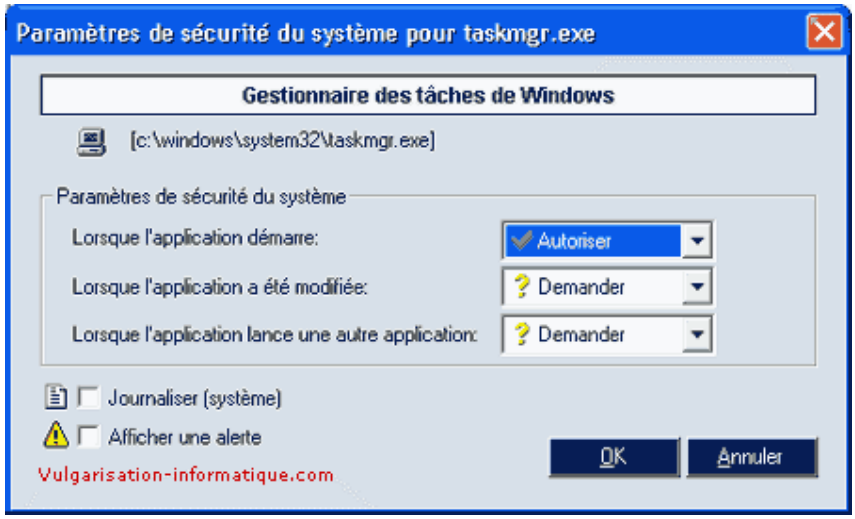
Pour ajouter une zone sécurisée, cliquez sur le bouton **ajouter**. Une fenêtre semblable à celle-ci s'ouvre :



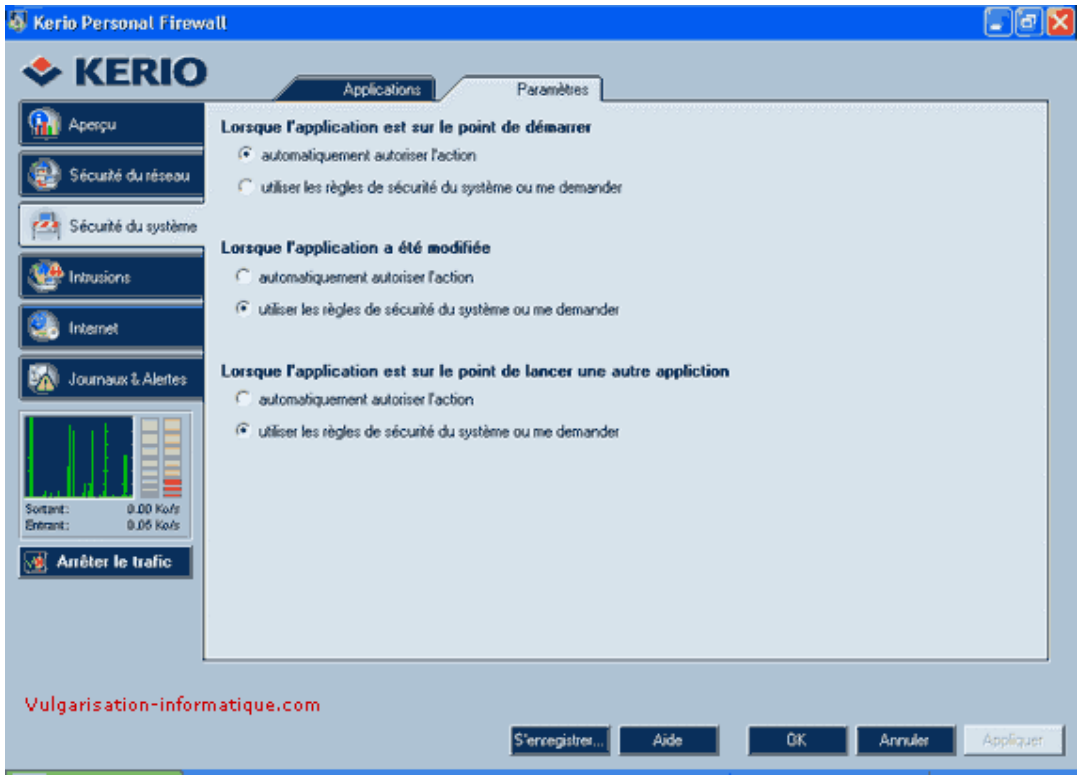
Ajoutez une description pour votre règle, sélectionnez **tous** pour le type de matériel. Dans la zone **type d'adresse**, sélectionnez une adresse ip ou une plage d'adresses ip. Cliquez ensuite sur **ok**, puis sur l'onglet **sécurité du système**.



Vous pouvez ici contrôler l'exécution des applications de votre PC. Double-cliquez sur l'application dont vous souhaitez modifier les droits. Vous arrivez face à une fenêtre de ce type :



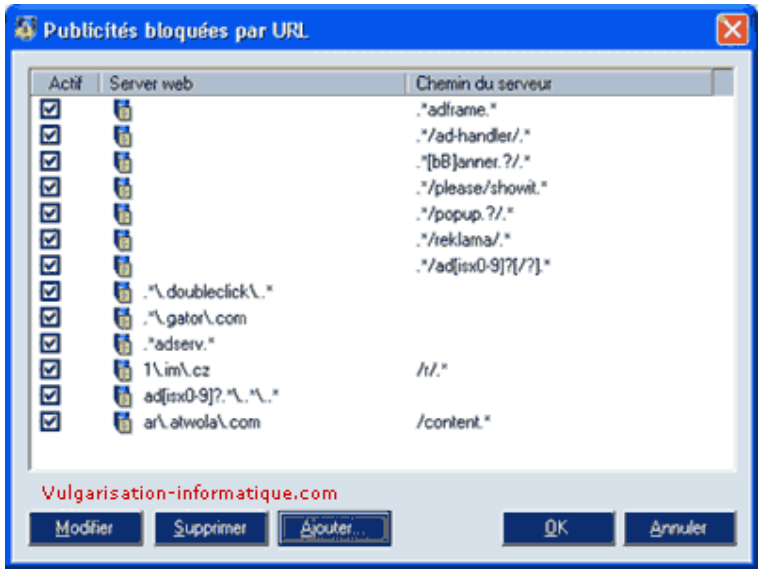
Modifiez ensuite les paramètres de l'application. Mettre **refuser** dans la zone **lorsque l'application démarre** empêchera l'application de démarrer. Cliquez ensuite sur **Ok**, puis sur l'onglet **paramètres**.



Pour un maximum de sécurité, sélectionnez pour la zone **Lorsque l'application est sur le point de démarrer**, l'option **Utiliser les règles de sécurité du système ou me demander**, de même pour la zone **Lorsque l'application est sur le point de lancer une autre application**. Cliquez ensuite sur l'onglet **intrusions**. Vous arrivez face à une fenêtre de ce type :

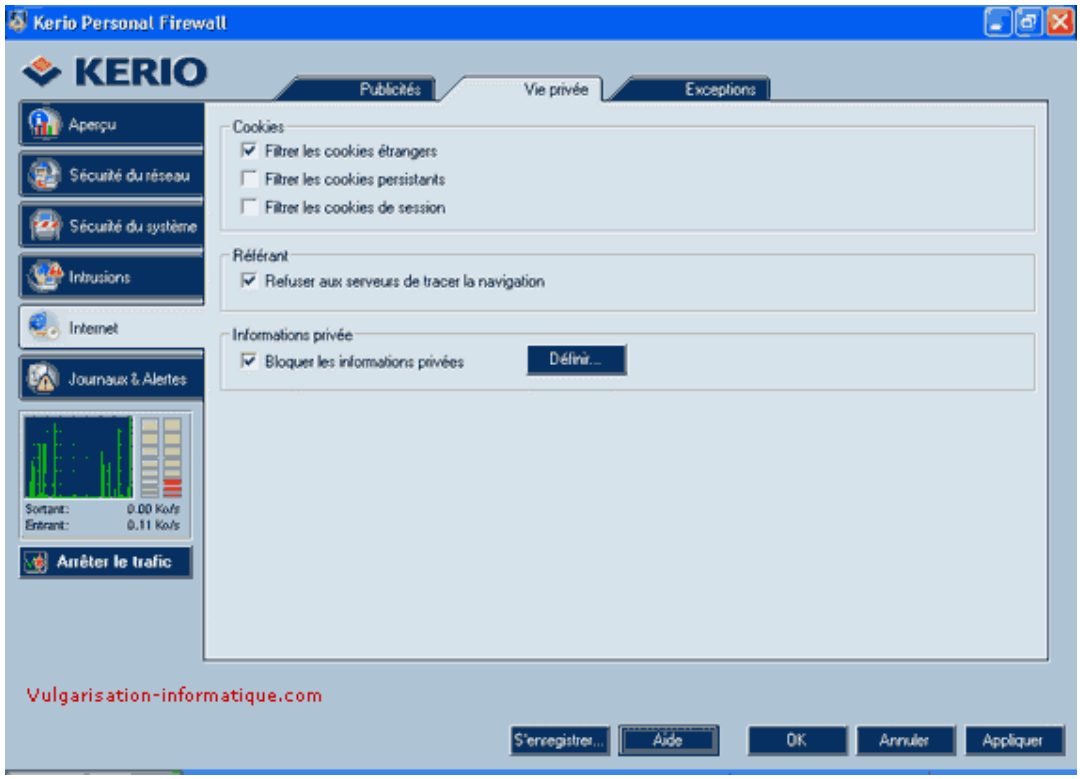
Mettez **Refuser** pour toutes les catégories d'intrusions, et cliquez ensuite sur l'onglet **internet**. Vous arrivez face à cet onglet :

Pour activer la protection web, cochez la case **activer le filtrage web**. Si vous cochez la case **bloquer les publicités**, vous pouvez ajouter des règles de blocage en cliquant sur le bouton **ajouter**. Vous pouvez aussi désactiver les règles initialement présentes.

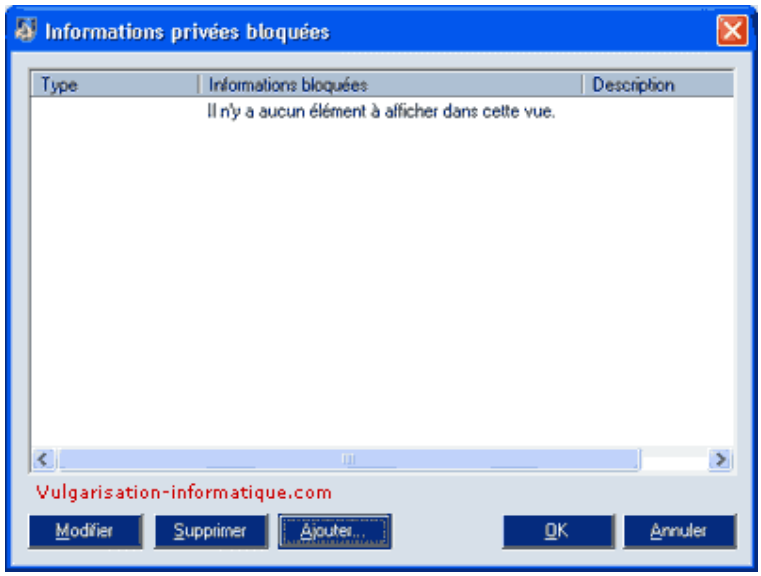


Le filtrage se base sur des caractères spéciaux ou des expressions régulières. Si vous pensez que les caractères spéciaux ne sont pas assez puissants pour définir la règle de filtrage que vous souhaitez, cochez la case **utiliser les expressions régulières au lieu des caractères spéciaux**. Une fois votre règle définie, cliquez sur **ok**.

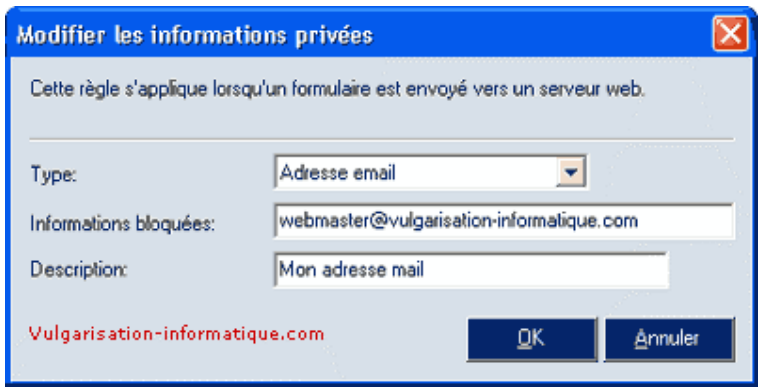
Cliquez ensuite sur l'onglet **vie privée** et cochez la case **filtrer les cookies étrangers**. Vous pouvez également cocher la case **refuser aux serveurs de tracer la navigation**. Cochez la case **bloquer les informations privées** et cliquez sur **définir**.



Vous arrivez face à un écran de ce type. Pour ajouter une information privée à bloquer, cliquez sur **ajouter**.

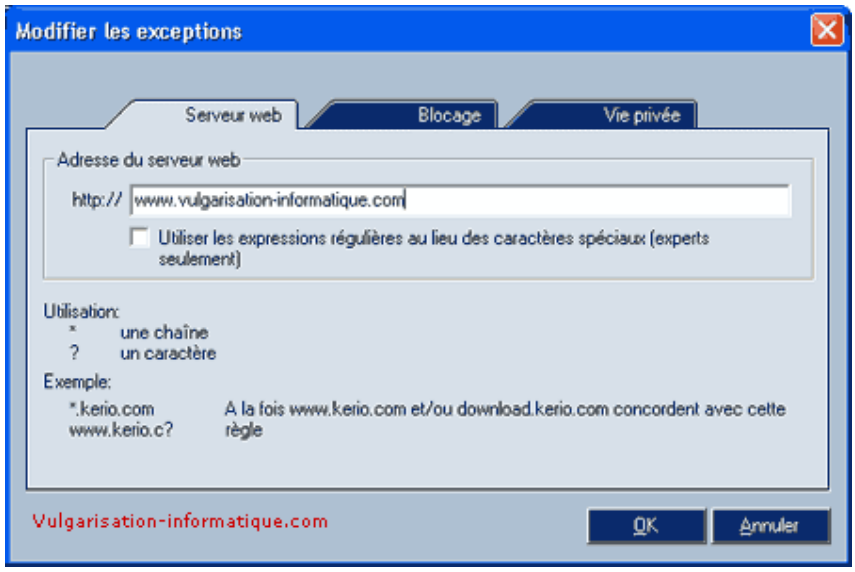


Vous pouvez alors choisir le type d'information à bloquer dans cette fenêtre. Une fois votre règle établie, cliquez sur **ok**.



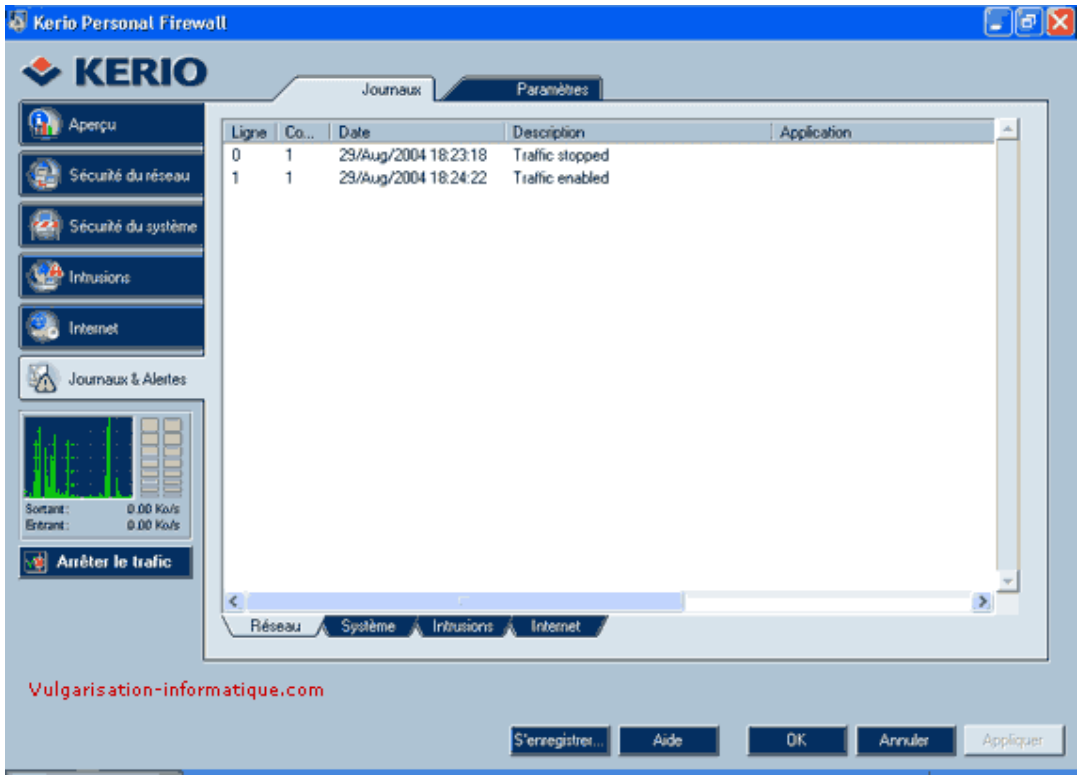
Cliquez ensuite sur l'onglet **exceptions**. Vous pouvez configurer ici des adresses web pour lesquelles vous pouvez définir des règles personnalisées.

Pour ajouter une règle, cliquez sur le bouton **ajouter**. Une fenêtre semblable à celle-ci s'ouvre :

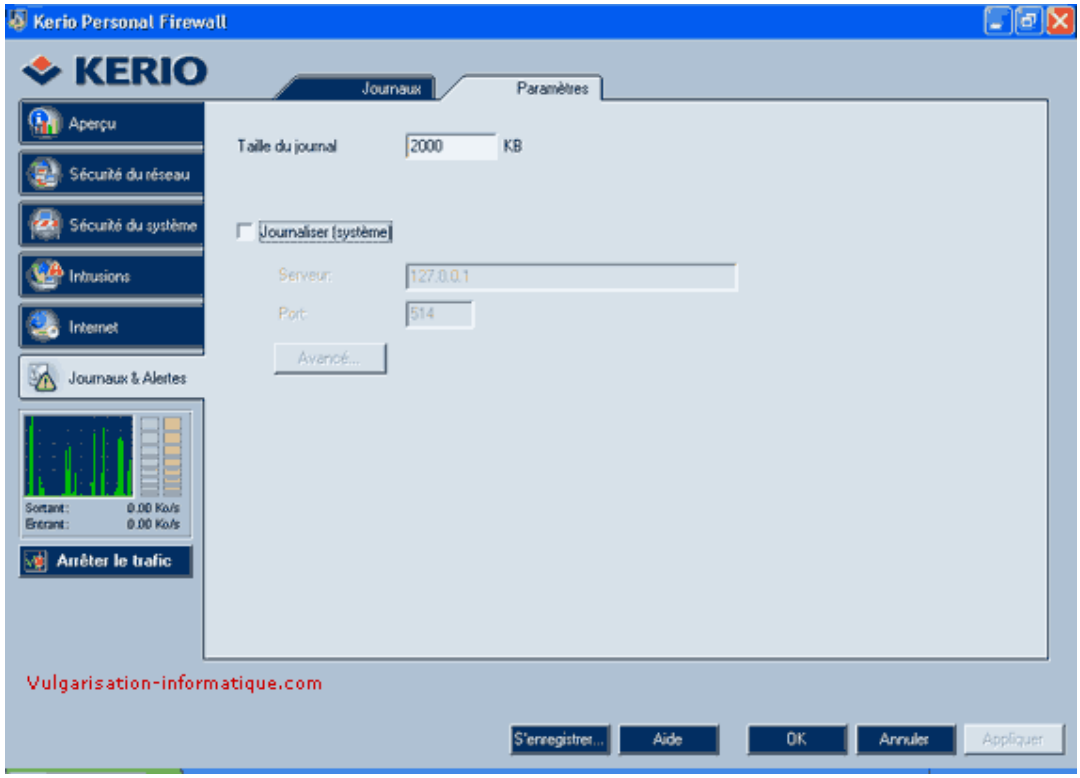


Le principe est le même : caractères spéciaux ou expressions régulières. Une fois l'adresse du site inscrite, cliquez sur **blocage** et ensuite sur **vie privée** pour configurer les paramètres comme si vous le faisiez globalement (vu précédemment)

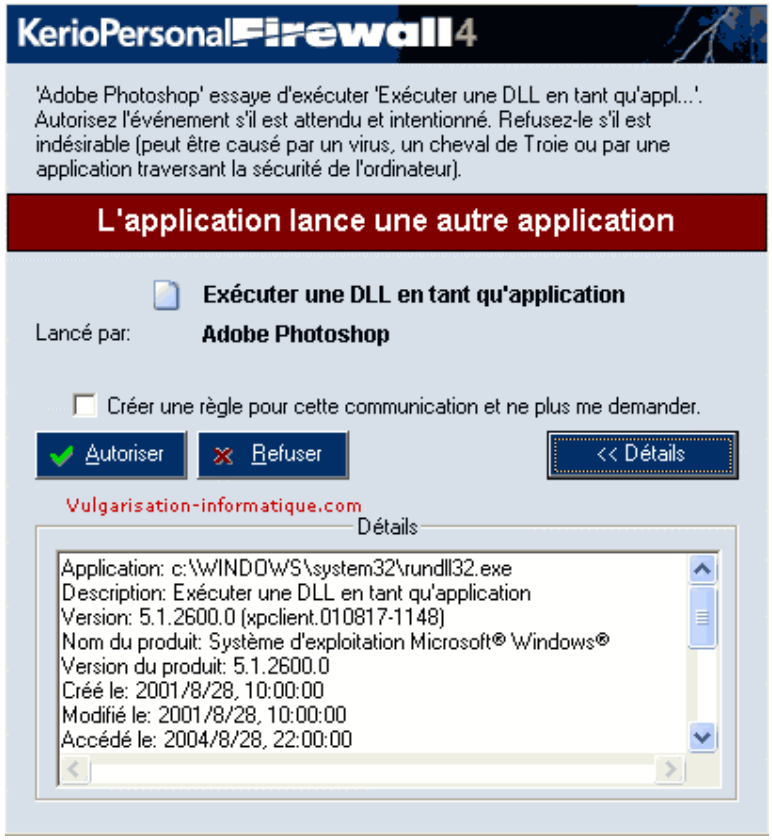
Cliquez ensuite sur l'onglet **journaux et alertes**. Vous pouvez consulter ici toutes les alertes et autres blocages effectués par Kerio.

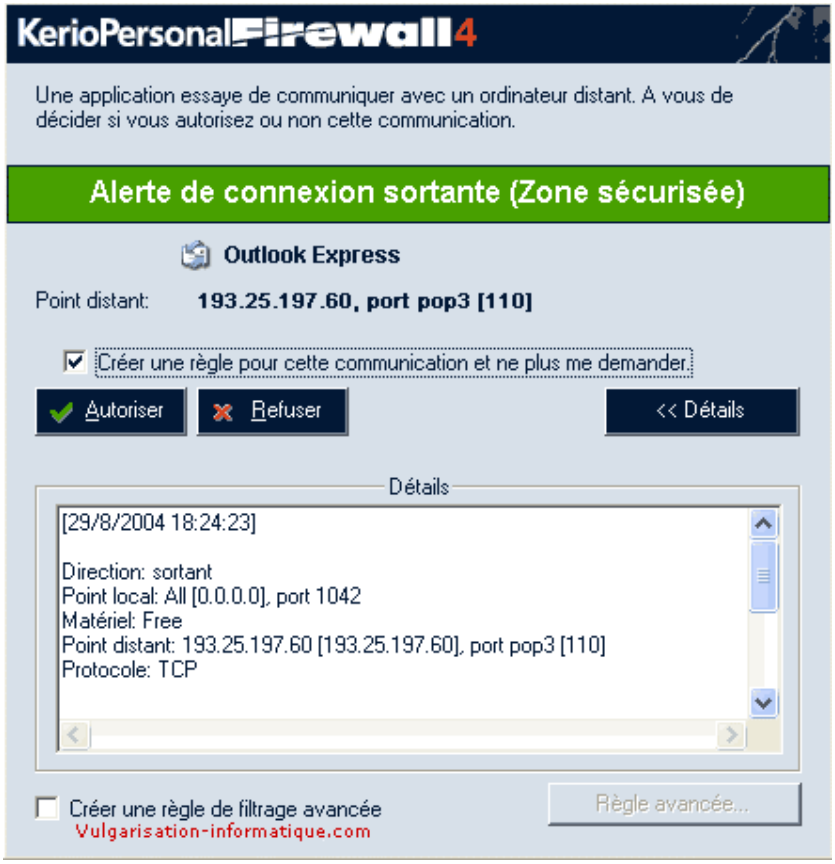


Cliquez sur l'onglet **paramètres** pour configurer la taille maximale du journal. Indiquer dans la case **taille du journal** une valeur de 2048 pour 2 Mo est une valeur correcte. Si vous souhaitez enregistrer les logs sur un serveur distant (ou local), cochez la case **journaliser(système)** et indiquez l'adresse ip et le port (par défaut 514) associé. Vous pouvez ensuite configurer ce qui est à journaliser en cliquant sur le bouton **avancé**.



Lorsque Kerio vous alerte, vous avez des écrans de ce type :





Vous pouvez alors cocher la case **créer une règle pour cette communication et ne plus me demander** pour ne plus recevoir d'alerte.

Barrer la route aux virus et aux vers avec Avast

Jadis cantonnés aux fichiers, les virus se logent aujourd'hui dans les mails, les pages Web et les logiciels que vous installez. Seule une surveillance permanente peut vous protéger.

Votre ordinateur se comporte étrangement, il fonctionne de façon anormalement lente ou vous constatez d'incessants accès au disque dur ? Il est possible que votre machine soit contaminée par un ver ou un virus. Aujourd'hui, un mode de propagation courant de ces hôtes indésirables est la banale pièce jointe aux courriers électroniques que vous recevez. Mais ce n'est pas le seul. Ainsi, des scripts peuvent se dissimuler dans les pages Web que vous affichez avec votre navigateur, et certains virus se cachent même dans des images au format JPeg. Pour vous protéger efficacement, il existe des antivirus gratuits tels que avast !, AVG et Antivir. A l'instar de leurs homologues commerciaux, ces logiciels disposent d'un module qui se charge en mémoire afin de vous protéger en permanence contre les virus, et d'un autre module permettant d'effectuer des analyses complètes de votre système à la demande.

Si vous pensez que votre ordinateur est infecté par un virus ou un ver, notez que certains éditeurs d'antivirus proposent gratuitement sur Internet des solutions immédiates d'analyse et de désinfection, comme le logiciel Housecall de Trend Micro que vous trouverez à l'adresse suivante : fr.trendmicro-europe.com .

Methodologie

Installez le logiciel antivirus avast !

Téléchargez avast ! à l'adresse telecharger.01net.com puis double-cliquez sur le fichier **setupfr.exe** pour l'installer. Suivez alors les instructions en sélectionnant la configuration **Typique.**

Une fois l'installation terminée, le programme vous propose d'analyser vos disques durs au prochain démarrage de votre ordinateur. Confirmez en cliquant sur **Oui.**

Configurez la protection de la messagerie

L'assistant de protection de messagerie s'ouvre alors. Cliquez sur **Suivant.** Cochez alors la case **Protéger automatiquement tous mes comptes,** puis sélectionnez l'option **Protéger automatiquement tous les comptes que je créerai dans le futur.** Cliquez ensuite sur le **Suivant.**

Déroulez la liste **Serveur SMTP** puis sélectionnez le serveur de messagerie que vous utilisez pour recevoir vos messages (cette information vous est donnée par votre FAI).

Faites alors de même pour le **Serveur Pop3 par défaut,** puis cliquez sur **Suivant** et sur **Terminer.** Enfin, redémarrez votre ordinateur.

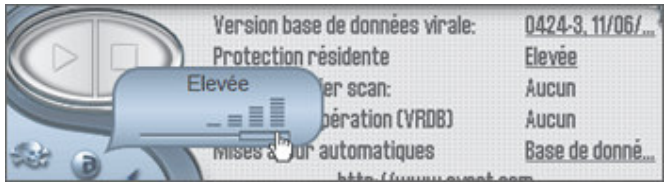
Mettez à jour les bases antivirales

Au démarrage suivant, avast ! vous indique qu'il est nécessaire de vous enregistrer afin de l'utiliser gratuitement. Cliquez sur le lien **Page d'enregistrement d'avast ! Edition Familiale.** Remplissez le formulaire. Vous recevrez, quelques minutes plus tard, une clé d'activation par mail. Lancez avast ! en double-cliquant sur l'icône **avast !Antivirus** qui se trouve sur le **Bureau.** Saisissez alors la clé que vous avez reçue par mail dans la fenêtre de dialogue **Enregistrer** puis validez par **OK.**

L'interface de contrôle d'avast ! s'ouvre alors. Cliquez sur le lien **Base de données** à côté de **Mises à jour automatiques.** Dans la fenêtre de réglages qui s'ouvre, cliquez sur le lien **Mettre à jour maintenant** de la rubrique **Base de données virale** et validez enfin par **OK.**

Optez pour une protection permanente

De retour sur l'interface principale, cliquez sur le lien **Désactivez** à côté de **Protection résidente.** Déplacez alors le curseur vers **Elevée.**



Tous les fichiers sans exception pourront ainsi être examinés en temps réel.

Analysez vos disques durs

Pour rechercher d'éventuels virus sur vos disques, cliquez sur l'icône **Disques locaux.** Dans la fenêtre qui apparaît, déplacez le curseur vers la droite afin de sélectionner l'option **Scan minutieux.** Puis cochez **Scan des archives** afin de vérifier les fichiers des archives compressées, et cliquez sur **Démarrer** pour débuter l'analyse.

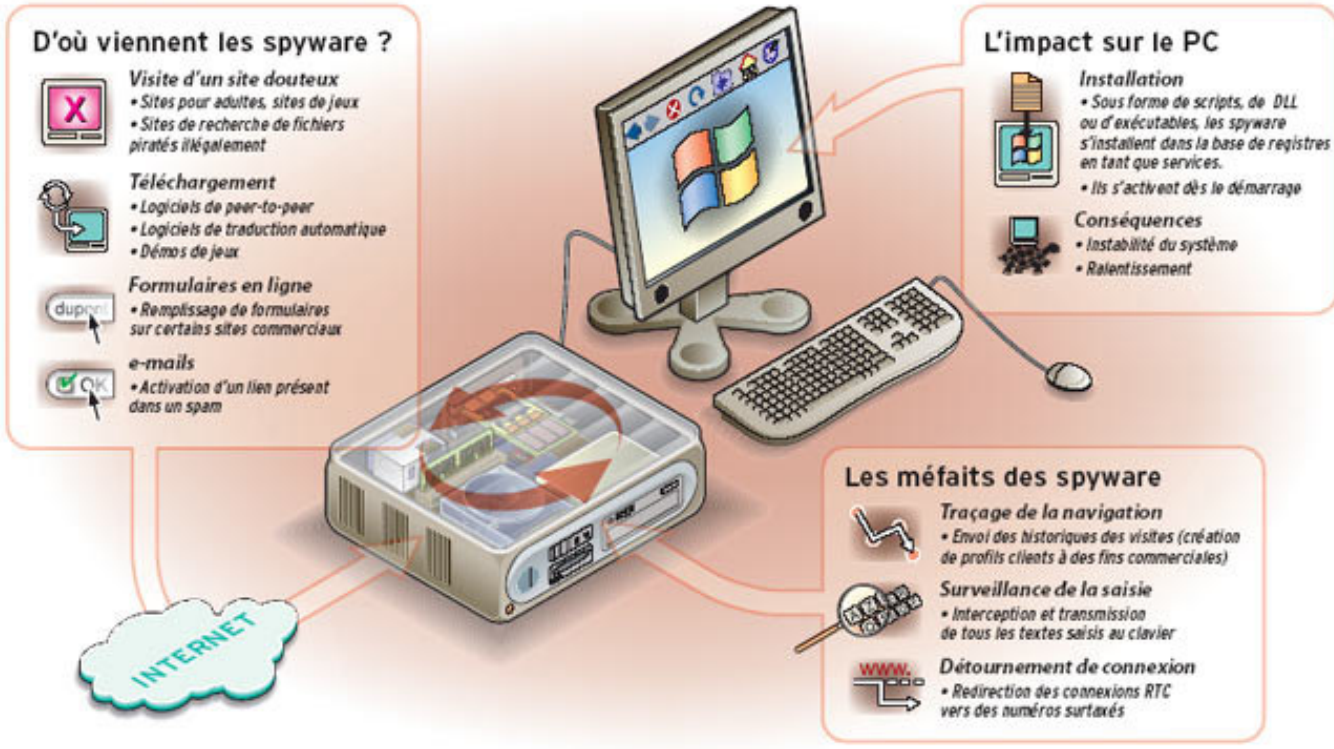
Supprimez un virus

Lorsqu'un virus est détecté, une fenêtre vous en informe et vous demande l'action à effectuer. Cliquez sur le bouton **Réparer** pour tenter de désinfecter le fichier contaminé.

Si la réparation est impossible, vous pouvez alors supprimer le fichier infecté ou bien le mettre en quarantaine pour l'envoyer ensuite au laboratoire de l'éditeur d'avast ! afin que celui-ci l'examine.

Eradiquer les logiciels espions installés avec Ad-Aware

Certains programmes récupérés sur Internet contiennent des logiciels espions qui permettent à leurs développeurs de connaître vos habitudes de navigation et ralentissent votre PC. Eliminez-les.



Dénomination	Particularités
PurityScan	Affiche des publicités sur les pop-up.
n-Case	Affiche des publicités.
Gator	Affiche des publicités.
CoolWebSearch	Redirige Internet Explorer vers des sites adultes et intercepte la saisie clavier.
Transponder	Analyse la navigation de l'internaute.
ISTbar	Détourne la page d'accueil et redirige vers des sites pour adultes.
PerfectNav	Analyse la navigation de l'internaute.
InternetOptimizer	Redirige vers la page d'accueil d'Optimizer.com
Perfect Keylogger	Enregistre la saisie clavier.
Dialer.Tibs	Invite à composer un numéro surtaxé pour se connecter à un site pour adulte.

Les logiciels espions, aussi appelés spywares, s'installent à votre insu et causent pas mal de dégâts : envoi à autrui de données confidentielles vous concernant, détournement de votre connexion à Internet, ouverture de failles de sécurité, altération de fichiers système, etc. Cette menace, relativement nouvelle, n'est pas toujours prise en compte par les programmes antivirus actuels. Pour vous en protéger, vous devez donc, en plus de votre antivirus, utiliser un logiciel antispyware comme Ad-aware SE Personal qui éradique les espions déjà présents

sur votre ordinateur et Microsoft Antispyware qui fait de même mais de manière complémentaire et qui en plus vous protége relativement en temps réel en empêchant certains espions de s'installer.

Ces deux programmes analysent la mémoire, puis examinent les fichiers de votre disque dur et le Registre de Windows à la recherche de logiciels suspects. Si l'outil détecte un programme espion, il peut le rendre aveugle, en d'autres termes l'empêcher de voir ce qui se passe sur votre ordinateur, ou tout simplement le détruire. Bien entendu, les logiciels anti-spywares demandent une mise à jour régulière de la base des espions détectés.

Methodologie

Installez et paramétrez Ad-Aware SE Personal

Téléchargez tout d'abord le logiciel antispyware Ad-Aware SE à l'adresse telecharger.01net.com . Double-cliquez ensuite sur le fichier **aawsepersonal.exe** pour lancer l'installation du programme. Lorsque celle-ci est terminée, vous pouvez choisir la langue de l'interface, en l'occurrence le français.

Pour cela, vous avez besoin du programme Ad-Aware SE Patch français que vous trouverez également sur le site telecharger.01net.com . Une fois le patch français installé, lancez Ad-Aware. Ouvrez la fenêtre de configuration du logiciel en cliquant sur l'icône symbolisant une roue dentée. Cliquez ensuite sur le bouton **Interface.** Déroulez alors la liste déroulante **Language File,** choisissez l'option **Français,** puis cliquez sur le bouton **Proceed.** Ad-Aware est désormais en français.

Mettez à jour la base de logiciels espions

Avant d'analyser votre système à la recherche d'espions, vous devez mettre à jour le fichier de définitions d'Ad-Aware qui contient les caractéristiques de tous les espions détectés. Cliquez pour cela sur le bouton **Statut.** Cliquez ensuite sur le lien **Vérifier les mises à jour.** Dans la fenêtre qui s'ouvre, cliquez sur le bouton **Connexion.**

Si une nouvelle mise à jour est disponible, Ad-Aware vous propose de la télécharger et de l'installer. Cliquez sur le bouton **OK** pour continuer. Une fois le téléchargement terminé, cliquez enfin sur le bouton **Terminer.**

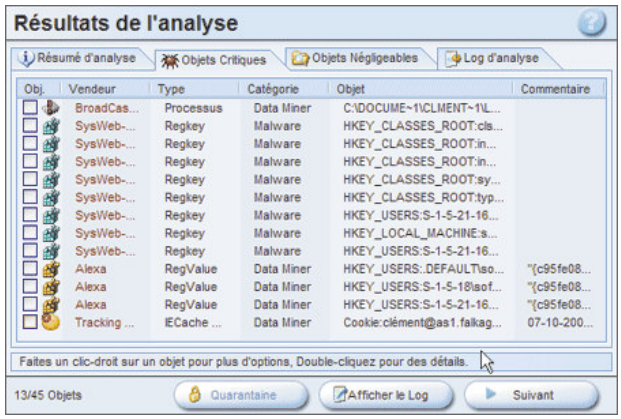
Lancez l'analyse

Cliquez sur **Analyser** pour démarrer un nouvel examen de votre système. Les paramètres par défaut conviennent. Cliquez sur **Suivant** pour débuter l'examen de votre mémoire vive, de vos disques durs, et du Registre de Windows. Après quelques minutes, Ad-Aware affiche le nombre d'objets suspects qu'il a trouvé sur votre système.

Chassez les mouchards

Faites un clic sur **Suivant** pour afficher la liste détaillée des fichiers suspects trouvés sur votre ordinateur. Pour avoir plus d'informations sur un objet, double-cliquez dessus. Une fenêtre affichera, entre autres, une description de cet objet, ainsi que son niveau de risque.

Pour plus de sécurité, éliminez les objets trouvés par Ad-Aware. En cas de problème, vous pourrez toujours restaurer un objet supprimé grâce au gestionnaire **Quarantaine** (accessible via un clic sur le bouton du même nom) qui sauvegarde automatiquement les éléments supprimés.



Cliquez donc n'importe où dans la liste avec le bouton droit de la souris, puis choisissez **Sélectionner tous les objets.** Cliquez ensuite sur **Suivant** puis sur **OK.** Les logiciels espions sont alors supprimés.

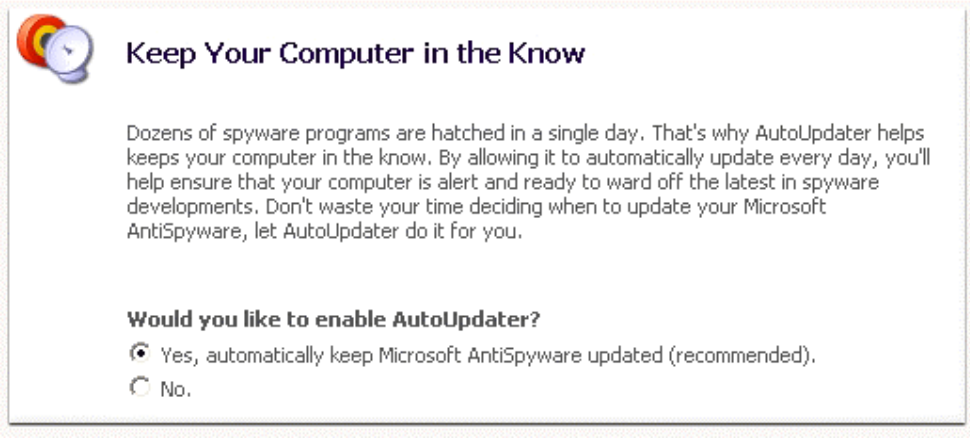
Protéger vous des logiciels espions avec l'antispyware de Microsoft

Télécharger le logiciel **Microsoft antispyware pour Windows** : http://www.clubic.com/telecharger-fiche136...ntispyware.html

Installer Microsoft antispyware, laisser les options par défaut.
Un raccourci est placé sur le bureau, via le menu démarrer, on peut aussi accéder au Microsoft AntiSpyware Update :

Lancer l'application, windows propose son **assistant de configuration** :

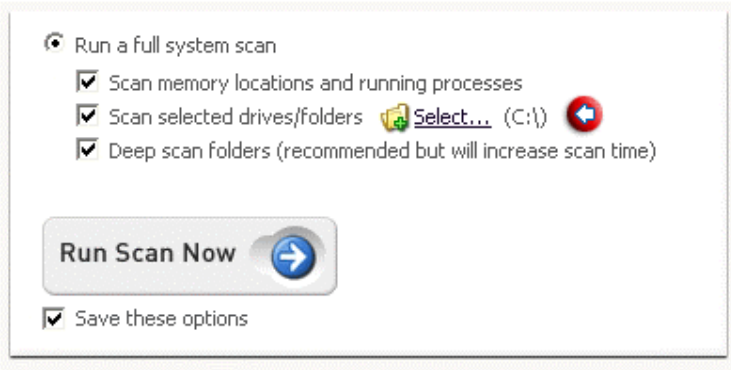
Confirmez que vous souhaitez des **mises a jour automatiques**:

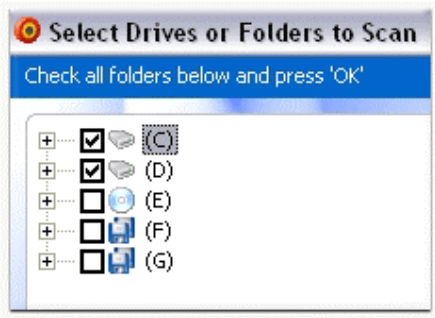


Le **Real-time security agent protection** tournera en tache de fond et analysera tout changement suspect dans vos logiciels :

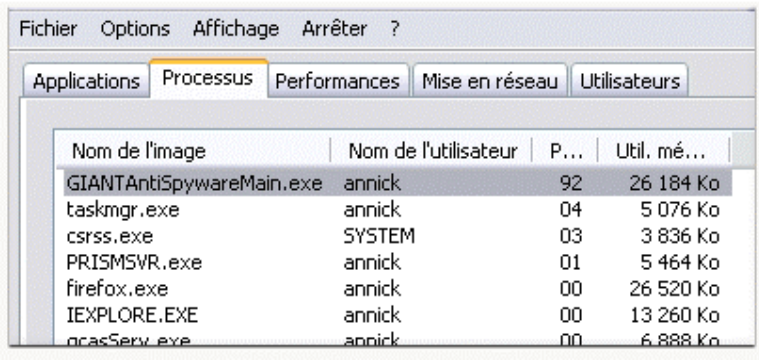
Cocher No

Une fois sur l'**interface d'administration**, le scan allégé est proposé par défaut.
Vous pouvez réaliser un scan plus complet en sélectionnant **Run a full system scan** puis en désignant tous vos disques durs:

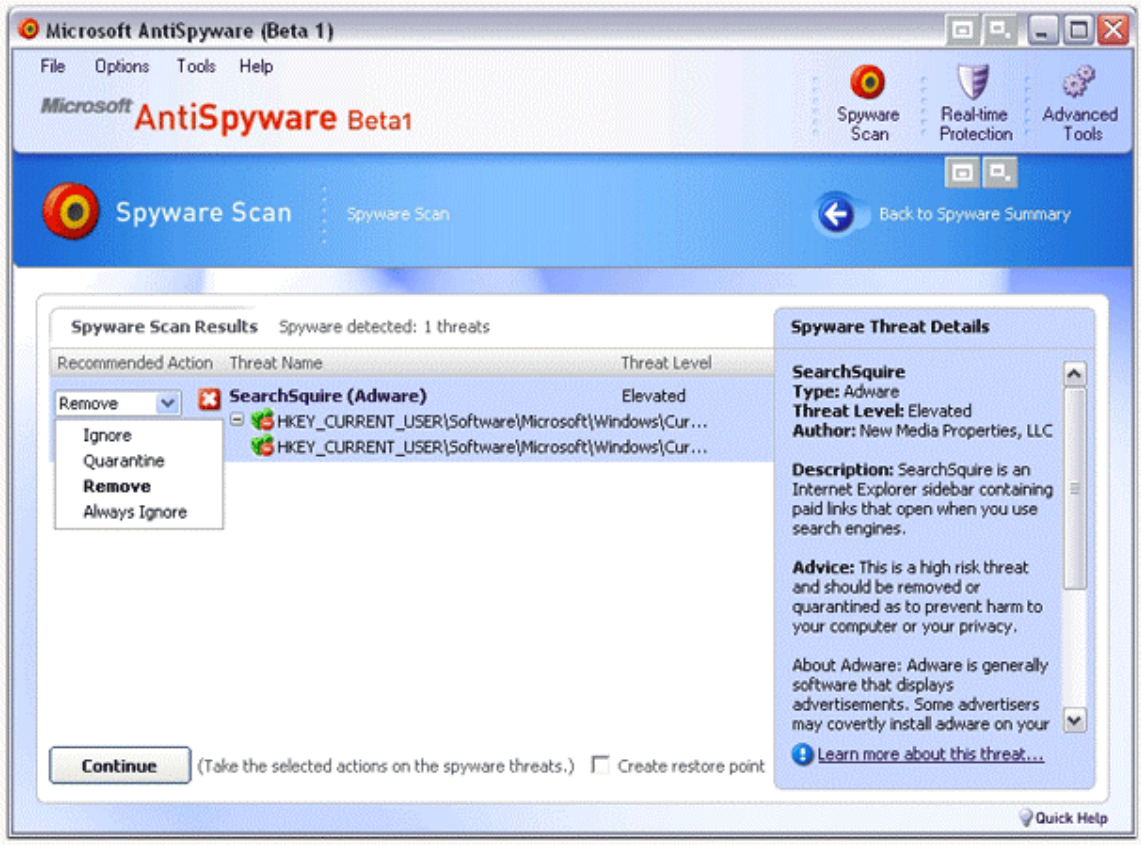




Pendant l'analyse on peut constater que les **ressources** occupées sont assez importantes (Testé sur un portable centrino 1.4 GHz).
L'utilisation d'un autre logiciel, meme de navigation internet, est passablement ralentie:



Après neuf minutes d'analyse, **Microsoft AntiSpyware** détecte une entrée dans le registre appartenant a une barre d'outils publicitaire.
C'est plutot une bonne performance, le pc concerné ayant été analysé quelques heures plus tot par le logiciel concurrent **Ad-Aware**:

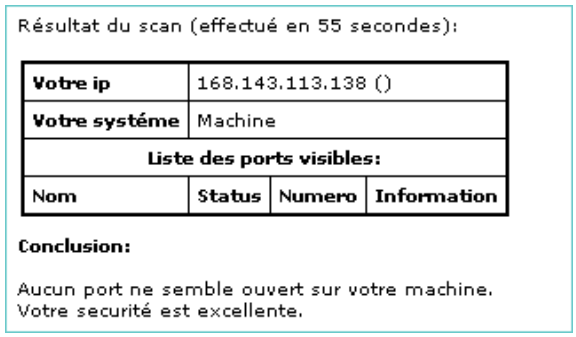


Confirmer la **suppression** du Spyware:

Décocher l'option Send to Spynet

Evaluer le niveau de sécurité du PC

Pour les informations qui voyagent entre votre ordinateur et l'extérieur (le Web), chaque logiciel utilisant Internet emprunte une ou plusieurs *« porte(s) numérotée(s) »* . Mais celles-ci peuvent aussi être empruntées par des personnes malveillantes voulant accéder à votre insu à votre micro depuis l'extérieur. Pour savoir s'il existe des portes ouvertes risquant de nuire à votre sécurité (et pour les identifier afin de les fermer avec un logiciel pare-feu, voir ci-contre), utilisez un service Web. Le site http://check.sdv.fr propose ce type de service. Depuis la page d'accueil du site, cliquez sur le bouton **Tester mon poste** . Après une ou deux minutes, un bilan de sécurité s'affiche.


Résultat du scan (effectué en 55 secondes):

Votre ip	168.143.113.138 ()		
Votre systéme	Machine		
Liste des ports visibles:			
Nom	**Status**	**Numero**	**Information**

Conclusion:

Aucun port ne semble ouvert sur votre machine.
Votre securité est excellente.

S'il signale des vulnérabilités, utilisez un logiciel pare-feu. Vous pouvez aussi vérifier le niveau de sécurité de votre ordinateur face aux attaques virales et aux dangers d'Internet, et vous informer sur les virus et risques du moment sur les sites www.symantec.com/region/fr et www.secuser.com .