SECTION INTERNET DU CLUB MEDERIC DE MARSEILLE

Internet Gazette

Site : http://aviquesnel.free.fr/Mederic

8 octobre 2007

Numéro 55

Sommaire

Joost s'ouvre enfin au public !

C'est officiel, Joost vient d'ouvrir ses portes public, mais toujours en beta. Depuis hier, la dernière version du logiciel est disponible sur le site de l'éditeur et la chaîne de téléchargement de Ratiatum.

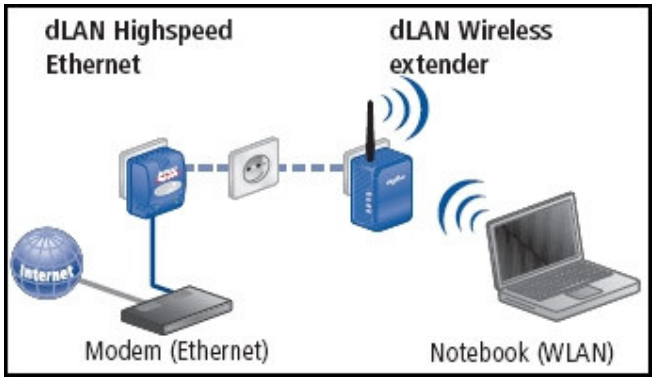
Outre le fait qu'elle ne requiert plus d'invitation pour l'utiliser, l'application a vu son interface complètement remaniée afin de la rendre plus attrayante. A noter la présence d'une nouvelle fonction intitulée "explore" qui permet d'intégrer un nouveau guide de chaînes les affichant par préférences. Mis à part cette amélioration dans le classement des chaînes, les évolutions de Joost 1.0 sont essentiellement esthétiques.

Etendre votre réseau domestique avec CPL + WiFi

Le dLAN Wireless extender de Devolo est un ensemble composé de deux adaptateurs CPL HomePlug avec interface sans fil qui réunit à la fois les avantages du dLAN et du WLAN. Le dLAN atteint théoriquement des débits de 85 Mbit/s et le WLAN, quant à lui, permet des débits de transmission de 54 Mbit/s (norme Wifi 802.11g).

L'ensemble permet de créer chez soi un accès sans fil à votre réseau dans chacune des pièces de votre maison ou appartement.

Concrètement, la mise en place se veut aisée : il suffit de brancher le premier adaptateur CPL sur une prise de courant et de le relier à votre ordinateur, modem, routeur ou encore sur la "box" de votre FAI. Il suffit ensuite de brancher le second adaptateur sur une seconde prise électrique dans une autre pièce afin d'avoir un nouveau point d'accès via câble Ethernet mais aussi Wifi. Enfantin !



Le bundle se compose des éléments suivants :

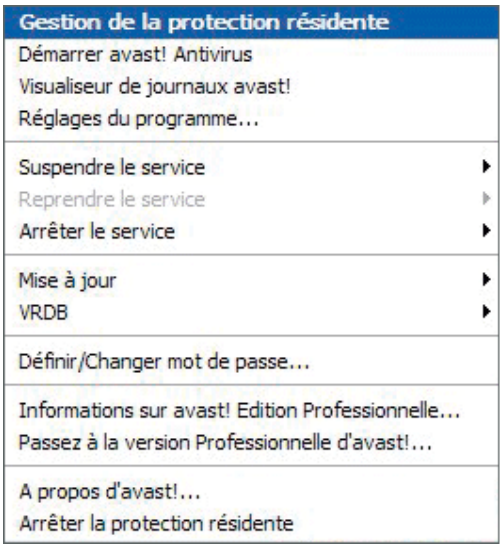
- un adaptateur CPL dLAN
- un adaptateur CPL Wireless
- un câble réseau RJ45
- un guide d'installation rapide
- un CD d'installation comprenant également les logiciels suivants (non obligatoires lors de l'utilisation du kit) :
    - *MicroLink EasyShare* : permet de partager des fichiers et des conversations à travers le réseau local.
    - *MicroLink Informer* : fournit des informations sur tous les périphériques dLAN dans votre réseau, par exemple leurs adresses MAC et les taux de transfert.
    - *MicroLink EasyClean* : permet de nettoyer les traces laissées par Internet Explorer.

Avast! : réglez le logiciel

Réglez le module principal de façon optimale

De prime abord, Avast! peut dérouter à cause de son interface différente de celle des autres antivirus. En effet, il la « découpe » en plusieurs modules. Le plus important est le module de protection résidente (il assure la protection en temps réel du micro), qu'il faut régler avec attention.

Cliquez du bouton droit de la souris sur l'icône d'Avast! en bas à droite de l'écran, et sélectionnez **Gestion de la protection résidente :**



Une fenêtre nommée **Scanner résident** s'affiche. Cliquez sur le bouton **Détails** pour avoir accès à tous les réglages.

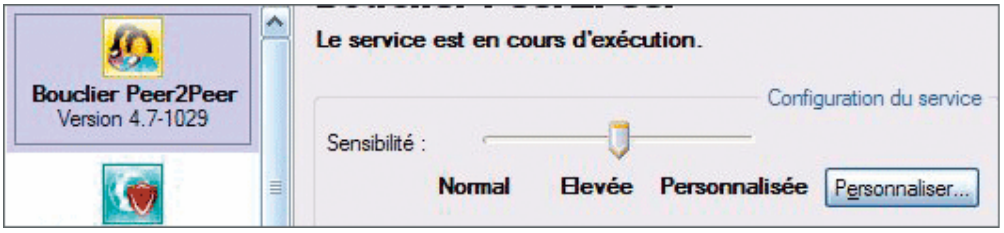
Nous allons détailler comment régler chacun des éléments (appelés boucliers). Une fois vos réglages effectués, cliquez sur **OK** pour fermer cette fenêtre.

Bouclier Peer2Peer

Cette protection n'est utile que si vous utilisez des programmes dits de *peer to peer,* comme BitTorrent ou TribalWeb.

Si ce n'est pas le cas, désactivez ce bouclier en cliquant sur le bouton **Terminer,** puis sur **Oui.** Pour réactiver un module désactivé, il suffit de cliquer sur le bouton **Démarrer,** situé sous le curseur du module, puis de confirmer par **Oui.**

Si vous utilisez ces logiciels pourvoyeurs de virus, réglez le curseur sur **Elevée.** Vous pouvez aussi cliquer sur **Personnaliser** afin d'adapter la surveillance aux seuls logiciels que vous utilisez.

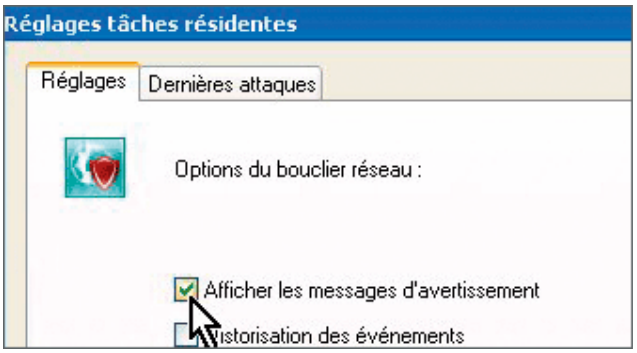


Dans la fenêtre qui s'ouvre, cochez ou décochez les cases correspondantes et cliquez sur **OK.**

Bouclier réseau

Ce bouclier empêche la propagation des virus provenant d'Internet vers les différents micros de votre réseau.

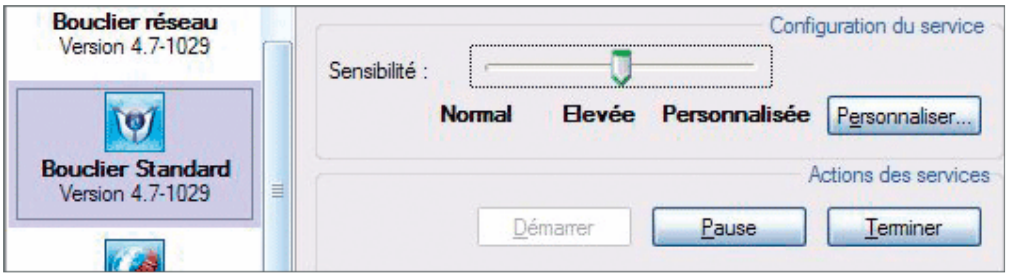
Il est inutile de changer son niveau de protection, car les options **Normal** ou **Elevée** ne changent rien à son fonctionnement. En revanche, il est possible d'afficher ou non les alertes éventuelles en cliquant sur le bouton **Personnaliser** , puis en cochant ou décochant la case **Afficher les messages d'avertissement.**



Bouclier Standard

Sa mission est d'analyser tous les logiciels ou fichiers qui sont lancés sur le PC.

S'il découvre un virus, il bloque son fonctionnement ou son ouverture. Choisissez l'option **Elevée** qui vérifie tous les fichiers alors que l'option **Normal** se contente des 57 formats les plus courants. Cela vous évite aussi de devoir vous perdre dans les nombreuses options de personnalisation. Enfin, il va de soi qu'il ne faut jamais désactiver ce bouclier... à moins d'avoir un bon motif pour le faire.

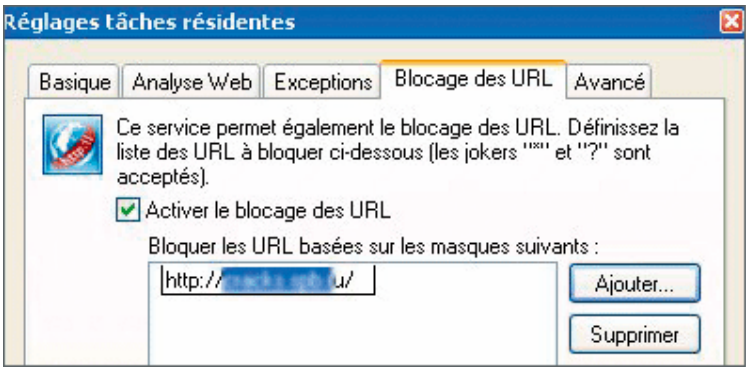


Bouclier Web

Ce bouclier est l'un des plus importants d'Avast! car il est en première ligne dans la lutte antivirale alors que le bouclier Standard n'est en quelque sorte qu'un second rideau de défense.

Il permet, par exemple, d'intercepter les virus cachés dans des archives aux formats Zip ou Rar avant même qu'elles ne soient téléchargées sur votre micro (là où d'autres antivirus ne les analysent que lors de leur ouverture). Le niveau de sensibilité qui s'impose est bien évidemment **Elevée.**

Ce réglage a pour effet d'activer toutes les options de personnalisation du bouclier. Mais vous pouvez tout de même aller plus loin dans la protection en interdisant l'accès à certains sites que vous savez pourvoyeurs de virus. Cela élimine définitivement le risque de télécharger par mégarde un fichier infecté de ce site ou, pire encore, de télécharger un fichier qui serait infecté par un virus encore inconnu d'Avast!. Pour mettre en place cette protection supplémentaire, cliquez sur le bouton **Personnaliser** puis sélectionnez l'onglet **Blocage URL.** Là, cochez la case **Activer le blocage des URL,** puis cliquez sur le bouton **Ajouter.** Tapez alors l'adresse du site en question et cliquez sur **OK.**



Désormais, si par erreur vous allez sur ce site, un message d'erreur s'affichera :

Courrier électronique

Ce module est destiné à vous protéger des risques liés à l'arrivée de virus via votre messagerie.

Ces infections sont parmi les plus fréquentes et les plus contagieuses, puisqu'elles peuvent se répandre via les carnets d'adresses. Il ne faut bien entendu jamais désactiver cette protection. Par défaut, elle est placée sur l'option **Normal,** ce qui est suffisant. Le placement du curseur sur **Elevée** aura pour seul effet d'augmenter à son niveau maximal la sensibilité **heuristique** de la détection, avec, comme gros inconvénient, un risque élevé de fausses alertes.

Parmi les autres réglages possibles, vous pouvez rassurer vos correspondants en faisant en sorte que les messages que vous leur envoyez affichent une information indiquant que le courriel a été vérifié par Avast! et qu'il est sain. Pour cela, cliquez sur le bouton **Personnaliser** puis, dans la fenêtre qui s'affiche, cochez la case **Insérer une note dans un message sain :**

Répétez l'opération avec les autres onglets nommés **SMTP** et **IMAP,** puis cliquez sur **OK.**

Messagerie instantanée

Ce module n'a d'intérêt que si vous utilisez un logiciel de messagerie instantanée tel que Windows Live Messenger ou encore Yahoo! Messenger.

Réglez la protection sur **Elevée,** puis cliquez sur **Personnaliser.** Dans la fenêtre qui suit, ne gardez que les cases cochées des logiciels que vous utilisez.

Si vous n'utilisez pas ce genre de logiciel, désactiver ce bouclier cliquant sur **Terminer,** puis sur **Oui.**

Outlook/Exchange

Ce bouclier n'est utile que si vous utilisez le logiciel de messagerie « professionnel » Outlook, livré avec la suite Office de Microsoft. Dans ce cas, réglez le curseur sur **Elevée.**

Si vous vous contentez de logiciels comme Outlook Express, Windows Mail, Windows Live Mail ou Thunderbird, vous pouvez désactiver ce module en cliquant sur le bouton **Terminer,** puis sur **Oui.**

Qu'est-ce que c'est ?

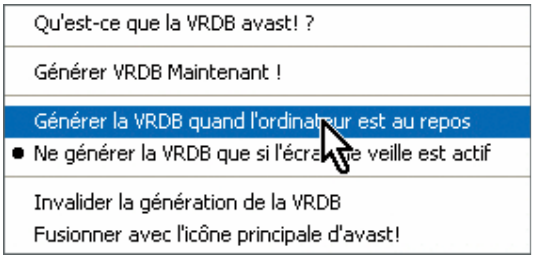
Heuristique

Méthode de détection des virus dont la signature n'est pas connue. L'analyse heuristique prend en compte le comportement des fichiers. Cette base d'analyse est sujette à plus d'erreurs que la méthode d'analyse sur base de données.

Réglez le fonctionnement de la VRDB

La VRDB, qu'est-ce que c'est ? Il s'agit d'une base de données, créée par Avast!, qui liste les fichiers présents sur le PC.

En cas d'infection sévère rendant un fichier inutilisable, son rôle est - comme son nom l'indique (VRDB signifiant *Virus Recovery Database)* -, de tenter de le remettre en l'état où il se trouvait avant l'infection. C'est pratique, mais gourmand en ressources. Le mieux est de cliquer du bouton droit de la souris sur l'icône de la VRDB (un petit **i** dans un rond bleu en bas et à droite de l'écran) pour sélectionner l'option **Générer la VRDB quand l'ordinateur est au repos.**

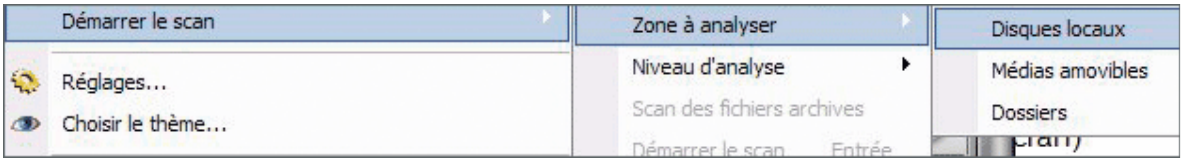


Vous pouvez aussi arrêter cette fonction en cliquant, dans la même liste, sur **Invalider la génération de la VRDB.** Enfin, profitez-en aussi pour faire disparaître l'icône de la VRDB en sélectionnant **Fusionner avec l'icône principale d'avast!**

Lancez une vérification manuelle

Quand vous souhaitez vérifier si un virus est présent sur un disque dur de votre ordinateur, cliquez avec le bouton de la souris sur l'icône d'Avast!, en bas à droite de l'écran, et sélectionnez **Démarrer avast! Antivirus.**

Dans la fenêtre principale du logiciel, cliquez n'importe où du bouton droit de la souris et sélectionnez **Démarrer le scan,** puis **Zone à Analyser** et enfin **Disques locaux.**



Pour une analyse très poussée, cliquez sur l'icône en forme de disque dur en haut à droite puis, dans la petite fenêtre qui s'affiche en haut, faites glisser le curseur vers **Scan Minutieux** et cochez la case **Scan des archives.**

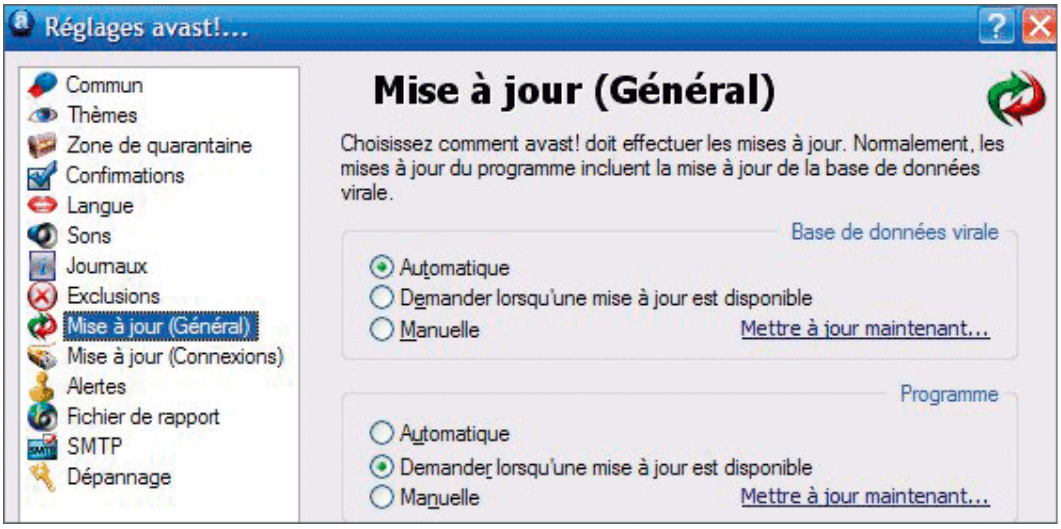
Cliquez n'importe où du bouton droit de la souris, et sélectionnez **Démarrer le scan** puis **Démarrer le scan.**

Accédez aux options

Pour modifier certains réglages, il faut passer par la fenêtre des options. Elle est accessible en cliquant du bouton droit sur l'icône d'Avast!, en bas à droite de l'écran, et en sélectionnant **Réglages du programme.** Deux éléments principaux sont à régler.

Vérifiez la périodicité des mises à jour

Dans le menu de gauche, sélectionnez **Mise à jour (Général)** et vérifiez qu'à droite les éléments sélectionnés sont bien **Automatique** pour **Base de données virale** et **Demander lorsqu'une mise à jour est disponible** pour **Programme.** Le cas échéant, vous pouvez choisir une autre option dans celles indiquées. Cliquez sur **OK.**



Avast! met à jour sa base de données de virus toutes les quatre heures.

Désactivez les alertes sonores

L'un des défauts d'Avast! est le dérangement régulièrement provoqué par les annonces de mise à jour de la base de virus ou du programme en lui-même. Pour supprimer ces alertes vocales pas très agréables, sélectionnez la ligne **Sons** dans le menu de gauche, puis cochez la case **Désactiver les sons d'avast!** .

Cliquez enfin sur **OK** pour valider.

Avast! : gérez la zone de quarantaine

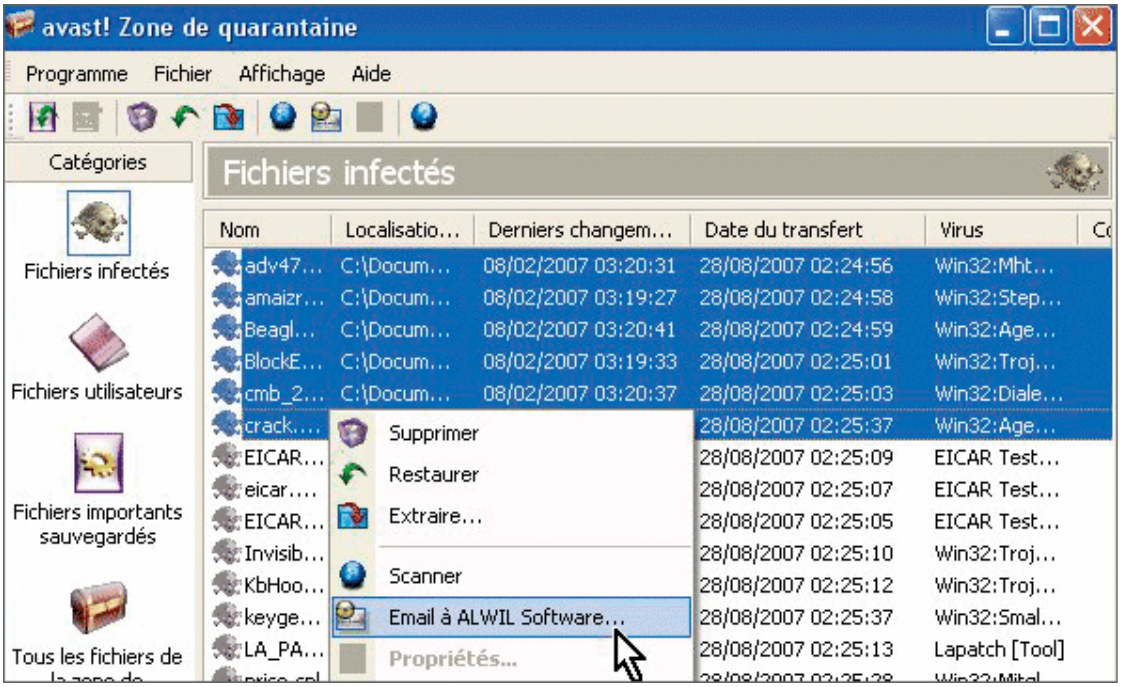
Lorsque l'antivirus détecte des fichiers infectés, il les place en quarantaine. Découvrez les possibilités offertes par cette zone particulière.

La zone de quarantaine sert à mettre à l'isolement tous les fichiers vérolés ou les fichiers désignés comme suspects. Elle offre quelques possibilités intéressantes. Pour y accéder, placez-vous dans la fenêtre principale d'Avast!, cliquez n'importe où du bouton droit de la souris et sélectionnez **Zone de quarantaine.** Le menu de gauche comporte quatre icônes :

Fichiers infectés

Quand vous cliquez dessus, la fenêtre affiche les fichiers vérolés qui ont été interceptés par Avast! et placés en quarantaine.

Cliquez sur un ou plusieurs fichiers avec le bouton droit de la souris pour accéder aux options.

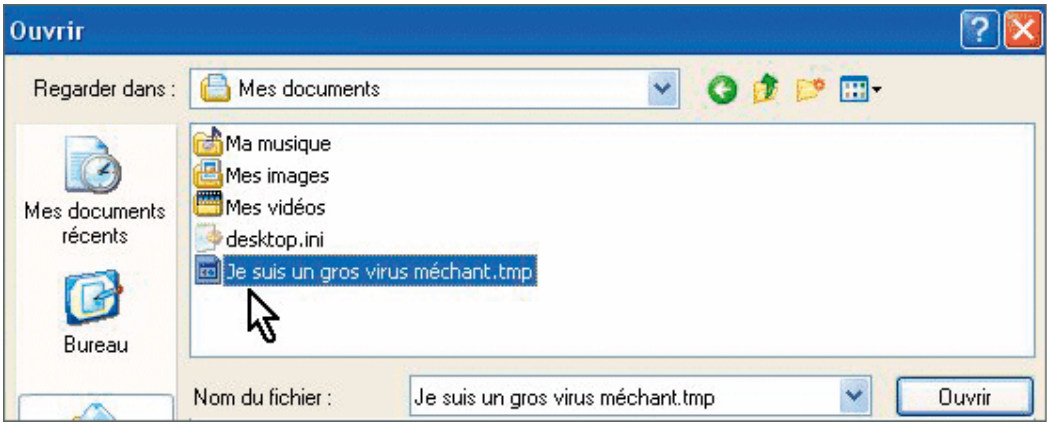


Vous pouvez, par exemple, définitivement supprimer un fichier, le scanner pour tenter de le nettoyer et, si l'opération est réussie, le restaurer à son emplacement d'origine.

Vous pouvez également envoyer un ou plusieurs fichiers infectés à l'éditeur d'Avast!, Alwil Software afin qu'il puisse analyser le virus contenu par ce fichier.

Fichiers utilisateurs

Cette icône donne accès à un espace qui vous permet de placer n'importe quel fichier suspect de votre choix en quarantaine. Pour cela, cliquez avec le bouton droit de la souris dans la partie droite de la fenêtre et sélectionnez **Ajouter.** Parcourez votre disque dur pour sélectionner le fichier désiré et cliquez sur **Ouvrir.**

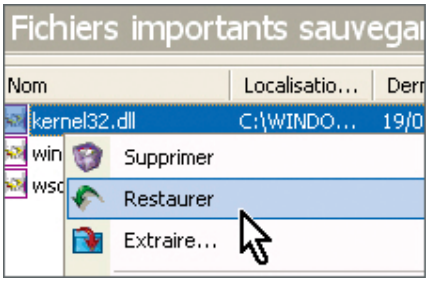


Cela peut être utile si vous n'êtes pas certain de l'intégrité d'un fichier, Même si Avast! ne lui trouve rien de dangereux.

Fichiers importants sauvegardés

Cette icône donne accès à des fichiers système de Windows considérés vitaux par Avast!. Le logiciel en a donc fait une copie lors de son installation.

L'intérêt est que, par un simple clic droit de la souris, vous pouvez restaurer l'un de ces fichiers en cas d'infection grave :



Tous les fichiers de la zone de quarantaine

Cette dernière icône récapitulative n'apporte pas de fonction de plus, puisqu'elle se contente de rassembler dans une seule fenêtre tous les fichiers de la quarantaine, qu'ils soient sains ou non

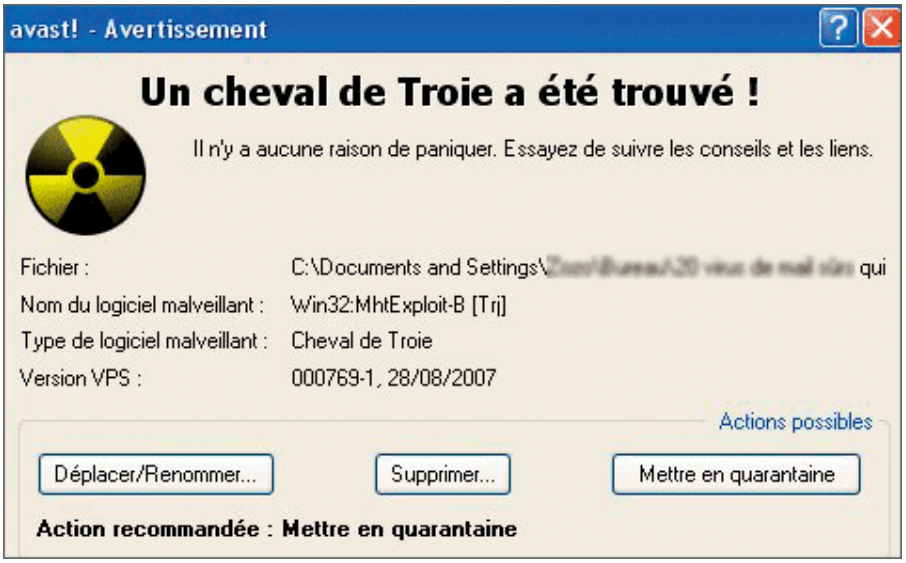
Avast! : réagissez aux alertes et aux messages

Dès que le logiciel détecte un virus, il vous en informe. Même chose lorsqu'il initie une mise à jour. Découvrez ces différents messages.

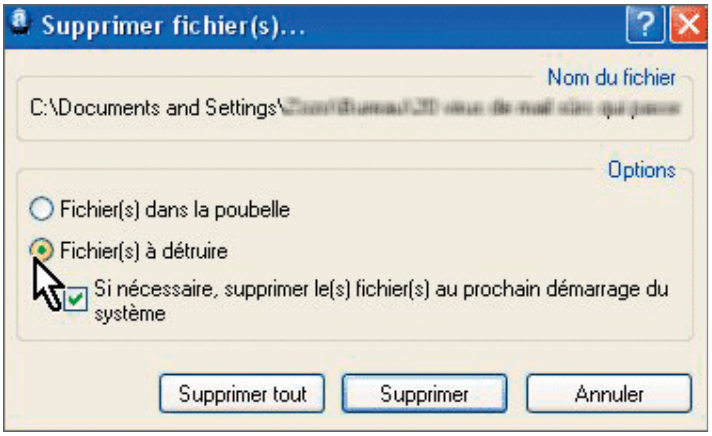
Les alertes

Cas numéro 1

Quand Avast! détecte un virus, il affiche un message clair sur l'écran et vous invite avec raison à ne pas paniquer. Trois choix vous sont alors proposés : **Déplacer/Renommer, Supprimer** et **Mettre en quarantaine.**



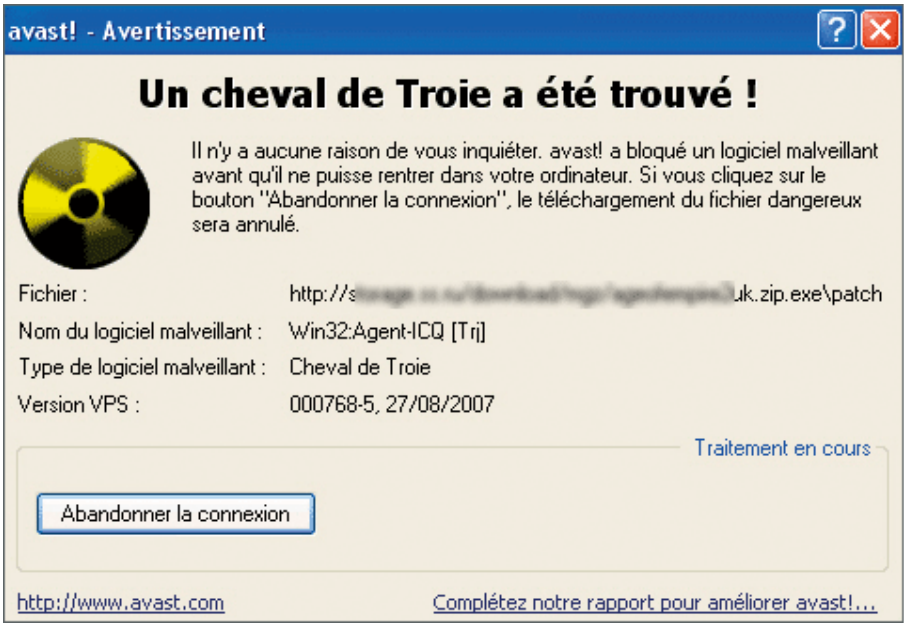
Si le fichier infecté ne vous dit rien ou s'il n'est pas important pour vous, il vaut mieux opter pour sa suppression en cliquant sur **Supprimer** et en cochant, dans la fenêtre qui suit, la case **Fichier(s) à détruire** puis en cliquant de nouveau sur **Supprimer.**



Si c'est un fichier important, il est préférable de choisir **Mettre en quarantaine.** Ainsi vous pourrez tenter de le désinfecter pour le récupérer par la suite via la **Zone de quarantaine.**

Cas numéro 2

Avast! peut aussi, lorsqu'il détecte l'arrivée d'un virus par votre liaison Internet (quand vous téléchargez un fichier par exemple), interrompre le téléchargement. La seule solution est alors de cliquer sur le bouton **Abandonner la connexion.**



Cas numéro 3

Si vous utilisez le logiciel de messagerie Outlook et qu'un correspondant vous envoie un courriel sans objet, il est possible qu'Avast! trouve ce message suspect et le bloque. Dans ce cas, vous pouvez choisir **Supprimer ce message** ou, si son expéditeur est sûr, l'accepter quand même.

Les messages

Cas numéro 1

Quand Avast! procède à la mise à jour de sa base virale, une boîte de dialogue bleue apparaît en bas à droite de votre écran :

Vous n'avez donc pas à vous inquiéter si ce message apparaît. Inutile également de cliquer dessus, vous n'avez rien à faire, tout est automatique. Le message disparaît au bout de quelques instants.

Cas numéro 2

Quand l'éditeur d'Avast! met en ligne une mise à jour de logiciel, une boîte de dialogue verte apparaît :

Là, en revanche, il faudra que vous cliquiez sur le message pour autoriser le téléchargement. Suivez alors les instructions, et cliquez sur **OK** pour valider et redémarrer votre micro.

Modifiez l'interface

La fenêtre principale d'Avast! est un peu déroutante et son aspect visuel n'est pas vraiment folichon. Elle est accessible en cliquant du bouton droit sur l'icône du logiciel, en bas à droite de l'écran et en sélectionnant **Démarrer avast! Antivirus !**

Il est fort heureusement possible d'en modifier l'aspect en cliquant du bouton droit de la souris sur la fenêtre d'Avast! et en sélectionnant **Choisir le thème.** Sélectionnez une ligne parmi celles proposées, et validez en cliquant sur **OK.** Vous pouvez aussi télécharger d'autres thèmes en cliquant sur le lien **D'autres thèmes sur notre serveur Web !**

Dans la page qui s'affiche, il vous suffit de choisir un thème et de cliquer sur **Télécharger** . Le fichier se placera non seulement au bon endroit sur le disque dur sans autre intervention, mais, en plus, il s'installera automatiquement pour changer l'apparence d'Avast!

Renforcez la protection avec BitDefender

La version gratuite de BitDefender ne suffit pas à protéger un ordinateur. En revanche, c'est un excellent complément à Avast.

Régulièrement bien placé dans la liste des antivirus efficaces, BitDefender est gratuit. Mais il doit être utilisé comme logiciel d'appoint, en complément d'un autre antivirus, Avast! par exemple.

En effet, dans sa version gratuite, il est dépourvu de protection en temps réel. En revanche, c'est un excellent « purgeur » pour le cas où vous seriez infecté. Bien entendu, cette efficacité n'est réelle que s'il est lui aussi correctement réglé.

Nos explications concernent la version 7.2 de BitDefender, qui présente l'avantage d'être intégralement en français, fichier d'aide compris. Les versions suivantes, désormais plus répandues, ne sont plus disponibles qu'en anglais.

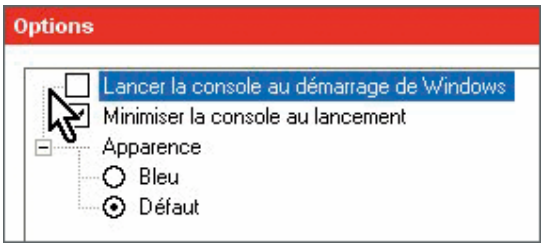
Etape 1 : Téléchargez BitDefender 7.2 Free Edition

1 - Lancez votre navigateur, et tapez l'adresse www.liens-utiles.fr/modules/wfdownloads/singlefile.php?cid= 46&lid=97.

Dans la page qui s'affiche, cliquez sur **Télécharger** puis, dans l'écran suivant, cliquez sur le bouton **J'accepte.**

Une fenêtre s'affiche : cliquez sur **Enregistrer,** sélectionnez le dossier où sera stocké le programme et cliquez sur **Enregistrer** pour démarrer le téléchargement.

2- Une fois le téléchargement terminé, ouvrez le dossier du disque dur où vous avez enregistré ce fichier, baptisé **bitdefender_free_win_v72.exe** et double-cliquez dessus. Suivez les instructions d'installation jusqu'au bout et redémarrez votre micro.



Etape 2 : Réglez le logiciel

Empêchez le lancement de BitDefender au démarrage

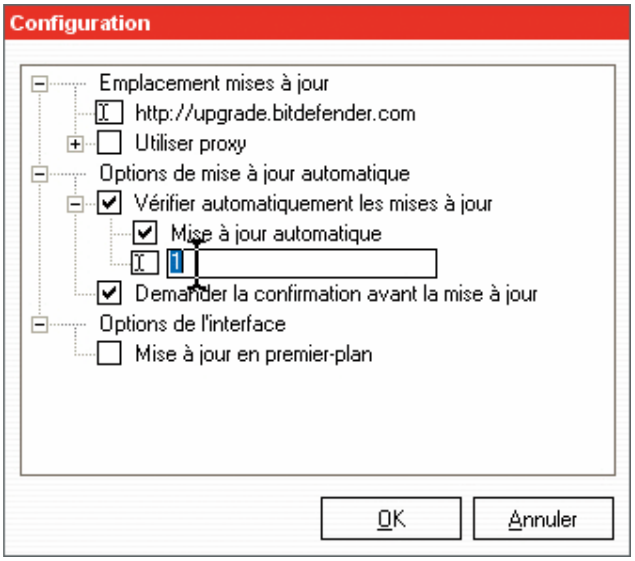
Même s'il ne possède pas de protection en temps réel, BitDefender se charge tout de même automatiquement au démarrage de l'ordinateur. Si vous ne voulez plus qu'il le fasse, par exemple pour réduire l'occupation en mémoire, cliquez du bouton droit de la souris sur l'icône de BitDefender qui se trouve en bas à droite de l'écran dans la **Barre des tâches** et, dans le menu qui s'affiche, cliquez sur **Options.**

Dans la fenêtre qui suit, décochez la case **Lancez la console au démarrage de Windows,** puis cliquez sur **OK** et redémarrez votre micro.

Modifiez la fréquence des mises à jour

Par défaut, les mises à jour de la base virale se font toutes les huit heures, ce qui n'est pas assez fréquent. Pour raccourcir ce délai, double-cliquez sur l'icône de BitDefender qui se trouve en bas à droite de l'écran dans la **Barre des tâches,** puis, une fois dans la fenêtre principale du programme, cliquez sur la ligne **Live! Update** .

Dans l'écran suivant, cliquez sur le bouton **Configuration** puis sur la ligne intitulée **Vérifier toutes les <8> heures.** A la place du chiffre **8** , tapez **1** pour une meilleure sécurité et cliquez sur le bouton **OK.**

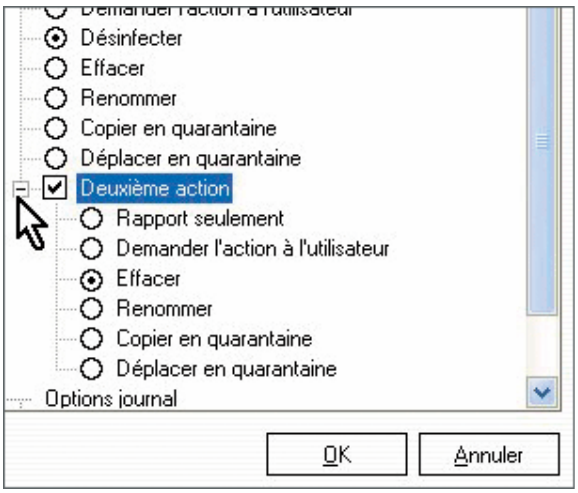


Dans la foulée, si vous voulez que BitDefender ne vous demande pas chaque fois s'il peut ou non télécharger et installer les mises à jour qu'il a trouvées, décochez la case **Demander la confirmation avant la mise à jour.**

Modifiez les options d'analyse

Les réglages de base font que, lorsqu'un virus est découvert, BitDefender tente d'abord de le nettoyer et, s'il n'y parvient pas, il le place en zone de quarantaine. Pour modifier ces choix, par exemple si vous préférez qu'un fichier non nettoyé soit systématiquement supprimé (ce qui est plus logique), ouvrez la fenêtre principale de BitDefender en double-cliquant sur son icône, en bas à droite de l'écran.

Cliquez sur la ligne **Virus Scan** puis, dans la fenêtre qui s'affiche, sur **Configuration.** Cliquez alors sur le signe **+** qui se trouve à la ligne **Deuxième action.** Dans la liste d'options qui s'affiche en dessous, sélectionnez celle intitulée **Effacer** et cliquez sur **OK :**



Planifiez une analyse du micro

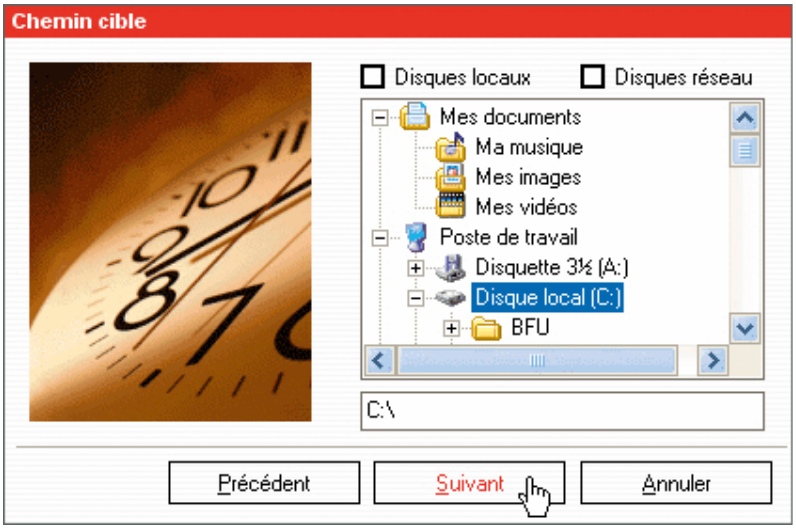
Que ce soit parce que vous n'utilisez pas votre micro à certaines heures ou parce que vous ne voulez pas être obligé de lancer manuellement des analyses, il est possible de planifier ces dernières soit pour une seule analyse, soit pour des analyses effectuées à intervalles réguliers.

Pour cela, depuis la fenêtre principale du programme, cliquez sur la ligne **Scheduler** puis sur le bouton **Créer.** Dans la fenêtre qui s'affiche, donnez un nom à la tâche et cliquez sur **Suivant.** Choisissez ensuite si la tâche doit s'effectuer une seule fois ou si elle doit se répéter. Dans le dernier cas, cliquez sur la ligne **Périodiquement.**

A ce moment, les différentes listes qui se trouvent en dessous deviennent actives.

Modifiez les données à votre convenance, par exemple en choisissant **Toutes les 1 semaines,** puis cliquez sur **Suivant** et faites de même dans la fenêtre suivante.

Dans la fenêtre qui suit, sélectionnez le disque dur à analyser (généralement **C:**) en cliquant dessus afin que sa lettre apparaisse dans l'espace texte qui se trouve sous le cadre.



Si vous avez plusieurs disques durs à faire analyser, cochez la case **Disques locaux** en haut, ce qui les sélectionnera tous, et cliquez sur **Suivant.**

Dans les quatre fenêtres suivantes, vous pouvez cliquer directement sur **Suivant** et, dans la dernière, qui résume tous les réglages sélectionnés, cliquez sur **Terminer** .

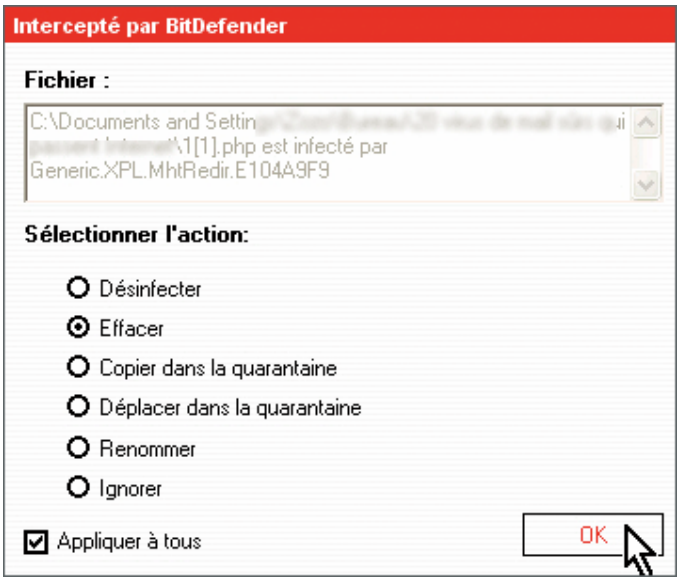
Etape 3 : Réagissez aux messages

Par défaut, BitDefender vous avertit s'il détecte une mise à jour à installer. Cliquez alors sur le bouton **OK** pour lancer l'opération. Si vous ne voulez plus être importuné par ces messages, décochez la case **Me demander avant de télécharger les mises à jour** avant de cliquer sur **OK.**

Notez tout de même que cela n'empêchera pas les mises à jour de se faire.

Etape 4 : Ce qu'il faut faire en cas d'alerte

Lorsqu'un virus est découvert, BitDefender vous demande ce qu'il doit faire. Si vous ne voulez plus qu'il pose cette question, il vous suffit, après avoir sélectionné l'option de votre choix parmi celles proposées (a priori **Effacer** ou **Copier dans la quarantaine),** de cocher la case **Appliquer à tous** et de cliquer sur **OK.**

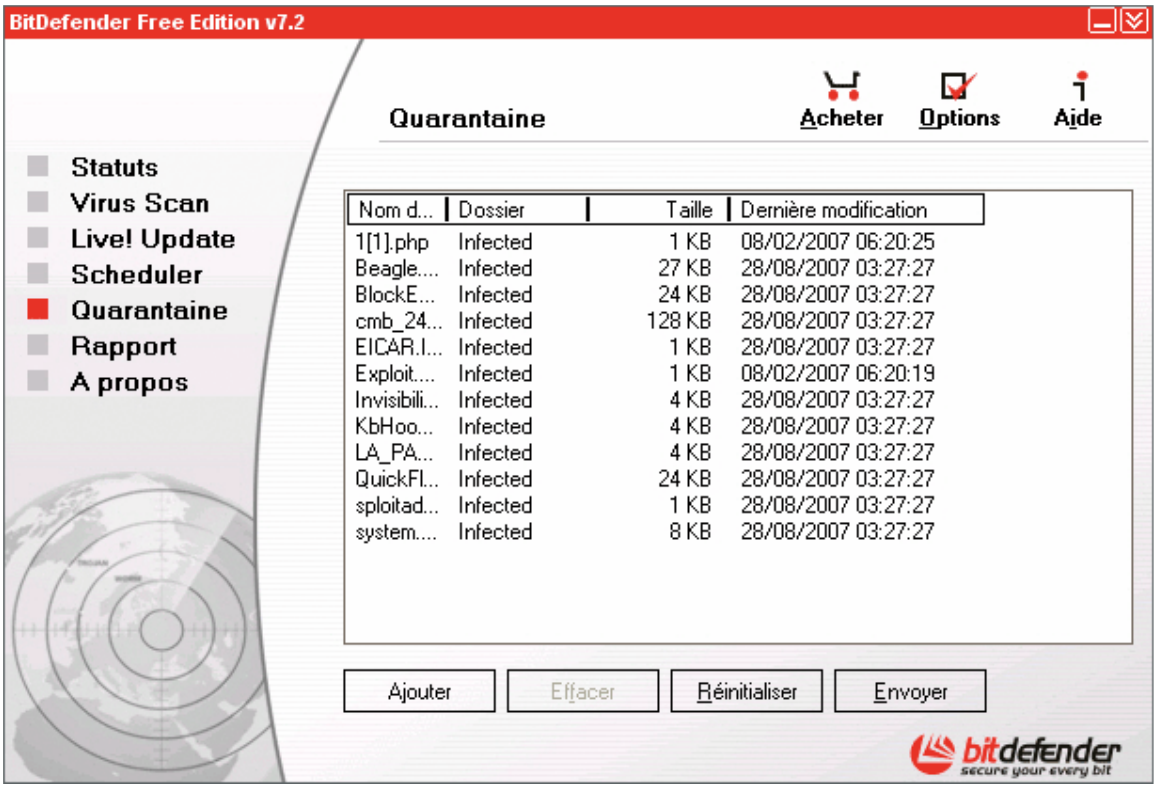


Ainsi, si d'autres virus sont découverts pendant cette analyse, ils subiront automatiquement le sort que vous leur avez réservé.

Etape 5 : Gérez la zone de quarantaine

Pour accéder à la zone de quarantaine où BitDefender stocke les fichiers infectés qu'il a trouvés, ouvrez la fenêtre principale du logiciel en double-cliquant sur son icône en bas à droite de l'écran. Cliquez sur la ligne **Quarantaine** pour faire apparaître la zone.

Lorsque vous l'affichez pour la première fois, elle est vide et ce, même si des virus vienent d'y être envoyés. Pour les faire apparaître, cliquez sur **Réinitialiser** .



Quand vous retournerez dans la zone de quarantaine, les fichiers que vous aurez fait apparaître seront visibles mais pas les éventuels « nouveaux venus » que vous aurez envoyés. Il faudra, chaque fois, utiliser le bouton **Réinitialiser**