bitdefender 9

Manuel d'utilisation

Antivirus

BitDefender 9 Standard
Manuel d'utilisation

SOFTWIN

Publié 2006.03.29
Build 9.5

Notice Légale


bitdefender
secure your every bit

Table des matières

Accord de licence

Cet accord de licence est un accord légal entre vous (entité individuelle ou utilisateur final) et SOFTWIN pour l'usage du produit de SOFTWIN identifié au-dessus, qui comprend le logiciel et qui peut comprendre les éléments média, les matériels imprimés et la documentation " en ligne " ou électronique (" BitDefender "), le tout étant protégé par la loi française et par les lois et les traités internationaux. En installant, copiant, ou utilisant de toute autre manière le logiciel BitDefender, vous acceptez les termes de cet accord. Si vous n'agréez pas les termes de cet accord, n'installez pas et n'utilisez pas BitDefender.

BitDefender est protégé par les lois du copyright et par les traités internationaux concernant le copyright, ainsi que par les autres lois et traités concernant la propriété intellectuelle. BitDefender est licencié et non pas vendu.

DROITS DE LICENCE. Ce logiciel restant la propriété de SOFTWIN, vous disposez néanmoins de certains droits d'utilisation une fois l'accord de licence accepté. Vos droits et obligations relatifs à l'utilisation de ce logiciel sont les suivants:

LOGICIEL. Vous pouvez installer et utiliser une seule copie de BitDefender ou de toute version antérieure sur le même système d'exploitation, sur un seul poste de travail. L'utilisateur principal de l'ordinateur, sur lequel BitDefender est installé, peut faire une copie additionnelle (seconde) pour son usage exclusif ou pour l'usage sur un ordinateur portable.

USAGE EN RÉSEAU. Vous pouvez emmagasiner ou installer une copie de BitDefender sur un dispositif de stockage, comme le serveur de réseau, employé seulement pour installer ou exécuter sur les autres ordinateurs d'un réseau interne ; néanmoins, vous devez acheter et dédier une licence séparée pour chaque terminal d'ordinateur sur lequel BitDefender est installé ou exécuté depuis le dispositif de stockage. Une licence de BitDefender ne peut pas être partagée ou utilisée de manière concurrentielle sur des postes ou terminaux d'ordinateurs multiples. Vous devrez acheter un pack de licences si vous en envisagez l'usage sur différents ordinateurs.

PACK DE LICENCES. Si vous achetez un Pack de Licences et que vous ayez acquis cet Accord de licence pour plusieurs licences de BitDefender, vous pouvez réaliser le nombre de copies du logiciel spécifié au-dessus comme "Copies licenciées". Vous avez aussi le droit de réaliser un nombre correspondant de copies pour l'usage sur des ordinateurs portables, comme spécifié ci-dessus dans la section "LOGICIEL".

TERMES DE LA LICENCE. La licence accordée ci-dessus commencera au moment où vous installez, copiez ou utilisez de toute autre manière BitDefender pour la première fois et continuera seulement pour l'ordinateur sur lequel le logiciel a été premièrement installé.

MISES À JOUR. Si BitDefender constitue une mise à jour, vous devez être correctement licencié pour utiliser le produit identifié par SOFTWIN comme étant éligible pour la mise à jour, afin d'utiliser BitDefender. Un produit BitDefender qui constitue une mise à jour remplace le produit qui formait la base de votre éligibilité pour la mise à jour. Vous pouvez utiliser le produit résultant seulement en accord avec les termes de cet Accord de licence. Si BitDefender est une mise à jour d'un composant d'un progiciel que vous avez acheté comme un seul produit, BitDefender peut être utilisé et transféré seulement comme une partie de ce progiciel et ne peut pas être séparé pour l'usage sur plus d'un ordinateur.

COPYRIGHT. Tous les droits d'auteur de BitDefender (comprenant mais ne se limitant pas à toutes les images, photographies, logos, animations, vidéo, audio, musique, texte et " applets " compris dans BitDefender), les matériels imprimés qui l'accompagnent et les copies de BitDefender sont la propriété de SOFTWIN. BitDefender est protégé par les lois concernant le copyright et par les traités internationaux. C'est pourquoi vous devez traiter BitDefender comme tout autre matériel protégé par le copyright à l'exception du fait que vous pouvez installer BitDefender sur un seul ordinateur, vu que vous gardez l'original seulement pour archive. Vous ne pouvez pas copier les matériels imprimés qui accompagnent BitDefender. Vous devez produire et inclure toutes les notices de copyright dans leur forme originale pour toutes les copies respectives du média ou de la forme dans laquelle BitDefender existe. Vous ne pouvez pas céder la licence, louer sous quelque forme que ce soit tout ou partie du logiciel BitDefender. Vous ne pouvez pas décompiler, désassembler, modifier, traduire ou tenter de découvrir le code source de ce logiciel ou créer des outils dérivés de BitDefender.

GARANTIE LIMITÉE. SOFTWIN garantit que le support sur lequel le logiciel est distribué est exempt de vices de matériaux et de fabrication pendant une période de trente (30) jours à compter de la date de livraison du logiciel. Votre seul recours en cas de manquement à cette garantie sera le remplacement par SOFTWIN du support défaillant durant la période de trente (30) jours à compter de la date de livraison du logiciel. SOFTWIN ne garantit pas que le logiciel répondra à vos besoins ni qu'il fonctionnera sans interruption ou sans erreur. SOFTWIN REFUSE TOUTE AUTRE GARANTIE POUR BITDEFENDER, QUELLE SOIT EXPRESSE OU IMPLICITE. LA GARANTIE CI-DESSUS EST EXCLUSIVE ET REMPLACE TOUTES AUTRES GARANTIES, QU'ELLES SOIENT IMPLICITES OU EXPLICITES, Y COMPRIS LES

GARANTIES IMPLICITES DE COMMERCIALISATION ET D'APPLICATION PARTICULIÈRE.

REFUS DES DOMMAGES. Toute personne qui utilise, teste ou évalue BitDefender admet les risques concernant la qualité et la performance de BitDefender. En aucun cas SOFTWIN ne sera tenu responsable à votre égard de tous dommages particuliers ou indirects, réclamations et pertes quelconques découlant de l'utilisation ou de l'incapacité d'utiliser le logiciel même si SOFTWIN a été avisé de l'éventualité de tels dommages.

NOTICE IMPORTANTE POUR LES UTILISATEURS. CE LOGICIEL N'EST PAS DÉSIGNÉ POUR DES MILIEUX DANGEREUX, DEMANDANT DES OPÉRATIONS OU UNE PERFORMANCE SANS ERREUR. CE LOGICIEL N'EST PAS RECOMMANDÉ DANS LES OPÉRATIONS DE NAVIGATION AÉRIENNE, INSTALLATIONS NUCLÉAIRES OU DES SYSTÈMES DE COMMUNICATION, SYSTÈMES D'ARMEMENT, SYSTÈMES ASSURANT DIRECTEMENT OU INDIRECTEMENT LE SUPPORT VITAL, CONTROLE DU TRAFFIC AÉRIEN, OU TOUTE AUTRE APPLICATION OU INSTALLATION OU LA DÉFAILLANCE POURRAIT AVOIR COMME EFFET LA MORT DES PERSONNES, DES BLESSURES PHYSIQUES SÉVÈRES OU DES DOMMAGES DE LA PROPRIÉTÉ.

RESTRICTIONS DE DROIT DU GOUVERNEMENT. Usage, duplication ou divulgation par le Gouvernement de BitDefender constituent sujet des restrictions stipulées par le sous paragraphe (c) (1) (ii) des Droits des Données Techniques et Software, clause DFARS 252.227-7013 ou sous paragraphes (c) (1) et (2) du Droit Commercial regardant le Software, clause 48 CFR 52.227-19. Contactez SOFTWIN au numéro 5, rue Fabrica de Glucoza, 72 322 - Sect. 2, Bucarest, Roumanie ou au Tél. 40-21-2330780 ou Fax : 40-21-2330763.

CONDITIONS GÉNÉRALES. Cet accord est régi par les lois de la Roumanie et par les règlements et les traités internationaux concernant le copyright. Cet Accord peut être modifié par une annexe de licence qui accompagne cet Accord ou par un document écrit qui ait été signé par vous et par SOFTWIN. Les prix, les coûts et les frais d'usage de BitDefender peuvent changer sans que vous en soyez prévenu. Dans l'éventualité d'une invalidité de tout règlement de cet Accord, cette invalidité n'affectera pas la validité du reste de cet Accord. BitDefender et le logo de BitDefender sont des marques déposées de SOFTWIN. Microsoft, Windows, Excel, Word, le logo de Windows, Windows NT, Windows 2000 sont des marques déposées de la Corporation Microsoft. Toutes les autres marques appartiennent à leurs propriétaires respectifs.

Préface

Ce *Manuel d'utilisation* est destiné à tous les utilisateurs qui ont choisi BitDefender 9 Standard comme solution sécurité pour leur ordinateur personnel. Les informations présentées dans ce livret sont destinées aussi bien aux utilisateurs expérimentés en informatique qu'a n'importe quelle personne sachant utiliser Windows.

Ce *Manuel d'utilisation* vous guidera pas à pas dans le processus d'installation de BitDefender 9 Standard, il vous apprendra comment le configurer. Vous y apprendrez les méthodes d'utilisation de BitDefender 9 Standard, la méthode de mise à jour, de test et de personnalisation. Vous saurez tirer le meilleur de BitDefender.

Nous vous souhaitons un apprentissage agréable et utile.

1. Conventions utilisées dans ce livret

1.1. Conventions Typographiques

Plusieurs styles de texte sont utilisés dans ce livret pour une lisibilité améliorée. Leur aspect et signification sont présentés dans la liste ci dessous.

Apparaison	Description
`Exemples`	Les exemples et quelques données numériques sont imprimés avec des caractères séparés d'`un espace`.
http://www.bitdefender.com	Les liens URL pointent vers un emplacement externe comme un serveur http ou ftp.
<sav.bitdefender@editions-profil.fr>	Les adresses Email sont insérées dans le texte pour plus d'informations sur les contacts.
« Préface » (p. xiii)	Ceci représente un lien interne vers un emplacement à l'intérieur de ce document.
`Nom de fichier`	Les fichiers et répertoires sont imprimés en utilisant des caractères séparés d'`un espace`.

Apparaison	Description
option	Toutes les informations sur le produit sont imprimées en utilisant des caractères **Gras**.
"texte cité"	Les textes cités sont fournis en guise de référence.

1.2. Avertissements

Les avertissements sont des notes textes graphiquement marquées, offrant à votre attention des informations additionnelles relatives au paragraphe actuel.

Note

La note est une courte observation. Bien que vous puissiez l'omettre, les notes apportent des informations non négligeables, comme des fonctions spécifiques ou un lien à un thème proche.

Important

Cette marque requiert votre attention et il n'est pas recommandé de la passer. Habituellement, elle apporte des informations non critiques mais significatives.

Avertissement

Marque une information critique que vous devrez lire attentivement. Rien de négatif ne se passera si vous suivez les indications. Vous devriez le lire et le comprendre car cette marqué décrit une opération risquée.

2. Structure du livret

La documentation est divisée en cinque parties, contenant les thèmes majeurs : Installation, Description et fonctions, Console de management, Meilleurs conseils et Obtenir de l'aide . De plus, le glossaire et les appendices sont fournis pour clarifier différents aspects de BitDefender, desquels pourraient résulter des problèmes techniques.

Installation. Des instructions pas à pas pour installer BitDefender sur un poste. Un tutorial clair sur l'installation et la configuration de BitDefender 9 Standard. Elles débutent par les prérequis pour une installation réussie, vous serez guidé à travers le processus d'installation entier et lors de la première session. Finalement, la procédure de désinstallation est décrite au cas où vous auriez besoin de désinstaller BitDefender.

Description et Avantages. Une courte introduction à BitDefender. Cette partie explique ce qu'est BitDefender, qui sont SOFTWIN et sa Data Security Division. BitDefender 9 Standard sera présenté, ses fonctions, les composants du produit et les bases de son intégration et du mécanisme de filtrage.

Console de management. Description de la gestion basique et de la maintenance de BitDefender. Les chapitres couvrent le démarrage et la fermeture du processus, comment obtenir les informations de lancement, comment tester l'efficacité de l'Antivirus , comment effectuer des mises à jour et comment enregistrer BitDefender 9 Standard.

Meilleurs conseils. Etapes à suivre pour vous assurer un PC sans virus&spyware.

Obtenir de l'aide. Où regarder et à qui demander de l'aide si quelque chose ne se passe pas bien.

Glossaire. Le glossaire tente de vulgariser des termes techniques et peu communs que vous trouverez dans ce document.

3. Commentaires

Nous vous invitons à nous aider à améliorer ce livret. Nous avons testé et vérifié toutes les informations mais vous pouvez trouver que certaines fonctions ont changé. N'hésitez pas à nous écrire pour nous dire si vous avez trouvé des erreurs dans ce livret ou concernant toute amélioration que nous pourrions y apporter pour vous fournir la meilleure documentation possible.

Faites le nous savoir en nous écrivant à cette adresse <documentation@bitdefender.com>.

Installation

Chapitre 1. Installation du BitDefender 9 Standard

La section **Installation du BitDefender 9 Standard** de ce Manuel d'utilisation contient les thèmes suivants:

- Système requis
- Etapes d'installation
- Mise à jour majeure
- Supprimer, réparer ou modifier les fonctions de BitDefender 9

1.1. Système requis

Pour assurer un fonctionnement correct du produit, vérifiez avant l'installation que vous disposez de la configuration suivante:

- **Processeur minimum** - Pentium MMX 200 MHz
- **Espace disque minimum** - 40Mo
- **Mémoire vive minimale** - 64MB (128Mo recommandés)
- **Système d'exploitation** - Windows 98/NT-SP6/ME/2000/XP; Internet Explorer 5.5 (+)

1.2. Etapes d'installation

Localisez le fichier d'installation et double-cliquez dessus avec la souris. Cela lancera l'assistant d'installation, qui vous guidera à travers le processus d'installation:

Etapes d'installation:

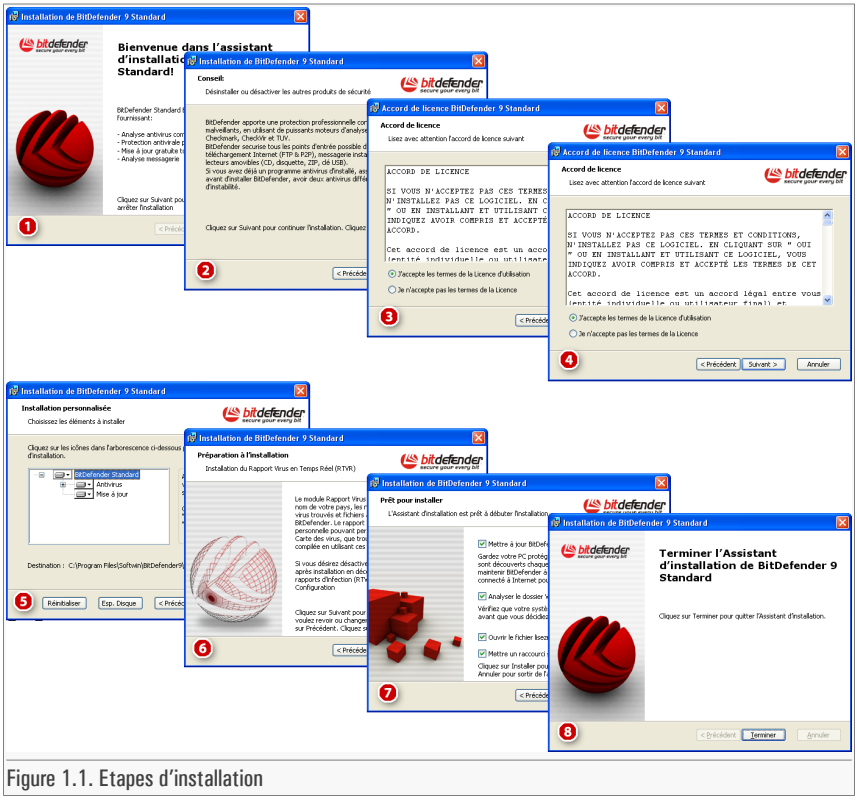

Figure 1.1. Etapes d'installation

1. Cliquez sur **Suivant** pour continuer ou sur **Annuler** si vous voulez quitter l'installation.

2. Cliquez sur **Suivant** pour continuer ou sur **Précédent** pour revenir à la première étape.

3. Merci de lire l' Accord de Licence, sélectionnez **J'accepte les termes de l'Accord de Licence** et cliquez sur **Suivant**. Si vous n'acceptez pas ces conditions, sélectionnez **Annuler**. Le processus d'installation sera abandonné et vous sortirez de l'installation.

4. Vous pouvez choisir quel type d'installation vous souhaitez : typique, personnalisée ou complète.

- **Typique** - Le programme sera installé avec les options les plus communes. Cela est recommandé pour la plupart des utilisateurs.
- **Personnalisée** - Cela vous donne la possibilité de choisir les composants que vous souhaitez installer. Recommandé pour les utilisateurs « avancés » uniquement.
- **Complète** - Pour l'installation complète du produit. L'ensemble des modules BitDefender seront installés.

  Si vous choisissez **Typique** ou **Complète** vous ne passerez pas par l'étape 5.

5. Si vous avez sélectionné **Personnalisé**, une nouvelle fenêtre apparaîtra, contenant la liste de tous les composants de BitDefender afin de pouvoir choisir ceux que vous souhaitez installer.

   Si vous cliquez sur l'un des composants, une courte description (incluant l'espace disque nécessaire) s'affichera sur le côté droit. Si vous cliquez sur l'un d'icônes une fenêtre apparaîtra où vous pouvez choisir d'installer ou non le module sélectionné.

   Vous pouvez sélectionner le répertoire dans lequel installer le produit. Le répertoire par défaut est `C:\Program Files\Softwin\BitDefender 9`.

   Si vous voulez choisir un autre répertoire, cliquez sur **Parcourir** et, dans la fenêtre qui s'ouvre, choisissez le répertoire. Cliquez sur **Suivant**.

6. Cliquez sur **Suivant**.

7. Vous avez quatre options sélectionnés par défaut:

   - **Mettre à jour BitDefender** - pour mettre à jour BitDefender à la fin de l'installation. Votre système doit être connecté à Internet pour cela.
   - **Analyser le dossier Windows System** - pour analyser le dossier système de Windows à la fin de l'installation.
   - **Ouvrir le fichier lisezmoi** - pour ouvrir le fichier lisezmoi à la fin de l'installation.
   - **Mettre un raccourci sur le bureau** - pour mettre un raccourci sur le bureau à la fin de l'installation.

   Cliquez sur **Installer** afin de commencer l'installation du produit.

8. Cliquez sur **Terminer** pour compléter l'installation du produit. Si vous avez accepté les paramétrages par défaut pour le répertoire d'installation, un nouveau répertoire du nom de `Softwin` est créé dans `Program Files` , contenant le sous-répertoire `BitDefender 9`.

Note
Il vous sera peut être demandé de redémarrer votre système pour terminer le processus d'installation.

1.3. Mise à jour majeure

La procédure de mise à jour majeure peut se faire de deux façons:

- Installez sans retirer la version précédente - v8 to v9

  Double-cliquez sur le fichier d'installation et suivez l'assistant décrit dans la section « *Etapes d'installation* » (p. 19).

Important
Durant le processus d'installation, un message d'erreur causé par le `Filespy service`, apparaîtra. Cliquez sur **OK** pour continuer l'installation.

- Désinstallez votre version précédente et installez la nouvelle

  Avant tout vous devez désinstaller la version précédente, redémarrer l'ordinateur et installer la nouvelle comme décrit dans la section « *Etapes d'installation* » (p. 19).

Important
Si vous mettez à jour v8 to v9 nous vous recommandons de sauvegarder les paramètres BitDefender. Une fois le processus de mise à jour est terminé, vous pouvez les recharger.

1.4. Supprimer, réparer ou modifier les fonctions de BitDefender

Si vous voulez modifier, réparer ou supprimer BitDefender 9 Standard, suivez le chemin depuis le menu Démarrer de Windows: **Démarrer** -> **Programmes** -> **BitDefender 9** -> **Modifier, reparer ou desinstaller**.

Il vous sera demandé confirmation de votre choix en cliquant sur **Suivant**. Une nouvelle fenêtre apparaîtra dans laquelle vous pourrez choisir:

- **Modifier** - pour sélectionner de nouveaux composants du programme à ajouter ou pour sélectionner des composants déjà installés et à retirer;
- **Réparer** - pour réinstaller tous les composants choisis lors de l'installation précédente;

Important

Avant de réparer le produit, nous vous recommandons de sauvegarder les paramétrages BitDefender. Dès que le processus de réparation est fini, vous pouvez les charger.

- **Supprimer** - pour supprimer tous les composants installés.

Pour continue le processus, sélectionnez l'une des trois options listées ci-dessus. Nous recommandons **Supprimer** pour refaire une installation. Après la désinstallation, supprimez le sous-répertoire `Softwin` dans le répertoire `Program Files`.

Description et Avantages

Chapitre 2. Vue d'ensemble

BitDefender vous apporte plusieurs solutions de sécurité pour satisfaire vos besoins en matière de protection des environnements informatiques actuels, proposant une gestion efficace des menaces à plus de 120millions de foyers et d'utilisateurs en entreprise dans plus de 100 pays.

Créé pour apporter une protection complète des réseaux et systèmes d'entreprise, la solution BitDefender comprend une protection antivirus, un antispam, un Firewall personnel et des solutions de gestion de la sécurité. BitDefender se spécialise aussi dans l'assistance en proposant des politiques de sécurité pour les réseaux d'entreprise.

BitDefender Professional a été le troisième produit de son genre dans le monde à recevoir la certification ICSA pour Windows XP et le premier à être primé pour son innovation par la Commission et Académies Européenne. L'Antivirus BitDefender est certifié par les organsimes majeurs du monde de la sécurité - ICSA Labs, CheckMark, CheckVir, TÜV et Virus Bulletin.

Softwin est localisé à Bucarest, Roumanie et possède ses bureaux à Tettnang, Allemagne, Barcelone, Espagne et en Floride, US. Site Web: http://www.bitdefender.com

2.1. Pourquoi choisir BitDefender?

Reconnu. Antivirus le plus réactif. La réactivité de BitDefender en cas d'épidémie de Virus a été confirmée en commençant par les derniers fracas de CodeRed, Nimda, Sircam et Badtrans.B ou d'autres codes malicieux à propagation rapide et dangereuse. BitDefender a été le premier à fournir des antidotes contre ces codes et à les rendre disponible gratuitement sur Internet pour toutes les personnes affectées. Maintenant, avec l'expansion rapide du Virus Klez – dans de nombreuses versions – une protection antivirus immédiate est devenue une fois encore vitale pour n'importe quel ordinateur.

Innovant. Primé pour son innovation par la Communauté Européenne et EuroCase. BitDefender a été proclamé vainqueur du prix IST Européen, remis par la commission Européenne et les représentants de 18 académies en Europe. Dans sa huitième année, le prix Européen IST est une décoration pour les nouveaux produits qui représentent le meilleur des innovations Européenne en matière de technologie d'information.

Simple. Couvre chaque point d'entrée potentiel, vous apportant une sécurité totale. La solution sécurité BitDefender pour les environnements professionnel remplit les conditions de protection des environnements de travail récents, permettant la gestion des menaces sérieuses qui planent sur vos réseaux, d'un réseau local de petite taille aux WAN multi plateforme en passant par les multiserveurs.

Votre Protection Ultime. La frontière finale à toute menace possible pour votre ordinateur. La détection de virus basée sur l'analyse de code n'a pas toujours prouvé son efficacité, BitDefender a implémenté une protection basée sur le comportement, apportant une sécurité contre les malware nouveaux nés.

Voici **les coûts** notre entreprise souhaite éviter et ce que nos produits sécurité sont destiné à empêcher :

- Attaque de Ver
- Perte de communication à cause d'e-mails infectés
- Dysfonctionnement de l'E-mail
- Nettoyage et restauration de systèmes
- Perte de productivité rencontrées par les utilisateurs finaux à cause d'indisponibilité du système
- Piratage et accès non autorisé causant des dommages

Certains **développements et avantages** simultanés peuvent être accomplis en utilisant la suite BitDefender :

- Amélioration de la disponibilité du réseau en stoppant la propagation des attaques de code malicieux(i.e., Nimda, Chevaux de Troie, DDoS).
- Protection à distance des utilisateurs contre les attaques.
- Réduction des coûts administratifs et avec les capacités de gestion et de déploiement rapide de BitDefender Enterprise.
- Stoppe la propagation de malware par e-mail, en utilisant la protection e-mail Bit-Defender sur le portail de la compagnie. Bloquez temporairement ou de manière permanente les codes non autorisés, et les connexions d'application coûteuses.

2.2. Data Security Division

Depuis le commencement, SOFTWIN's Data Security Division approche la protection de données de manière spécifique, avec la première mise à jour intelligente, ne requérant aucune intervention de la part de l'utilisateur,la première gestion antivirus à distance par la technologie WAP ou le premier Firewall personnel intégré au moteur

antivirus apportant une réponse complète aux menaces de sécurité complexes de nos jours.

Né pour apporter une sécurité totale des données à tous les niveaux critiques des environnement de travail actuels, Data Security Division vise à protéger les systèmes contre les virus d'ordinateurs, à faire la recherche antivirus , à développer de nouvelles technologies de surveillance de toutes les manières possibles d'infection d'un système et l'éducation publique des IT&C sur les dangers des virus informatiques.

Les solutions sécurité de BitDefender remplissent les conditions de protection des environnements de travail récents, permettant une gestion des menaces sérieuses qui planent sur vos réseaux, d'un réseau local de petite taille aux WAN multi plateforme en passant par les multiserveurs.

2.3. SOFTWIN

La société SOFTWIN basée à Bucarest est le fournisseur pionnier de solutions logicielles complexes et de services en Roumanie.

SOFTWIN se concentre sur le développement de solutions logicielles et de services qui permettent aux entreprises grandissantes de résoudre leur challenge critique d'activité et de capitaliser sur de nouvelles opportunités de commerce.

SOFTWIN permet aux compagnies de se concentrer sur leur activité principale et de s'étendre vers de nouveaux marchés en se débarrassant des problèmes mineurs.

SOFTWIN emploie plus de 500 professionnels hautement qualifié et expérimentés dans le développement de solutions personnalisées et de services.

Depuis sa création en 1990, le revenu annuel moyen de SOFTWIN s'accroît de 30%.

SOFTWIN possède 4 divisions, qui définissent aussi les grandes lignés d'activité de la compagnie :

- CRM
- Solutions d'Information Business
- Solutions de contenu Electronique
- Solutions de sécurité de Données

SOFTWIN apporte mondialement des services et des solutions à ses clients. Plus de 90% des turnover de compagnie s'effectue lors de l'exportation aux US et dans l'union Européenne.

En utilisant des technologies de pointe, SOFTWIN a créé brillamment plus de 500 projets de développement de logiciels, plus de 3,500 projets structurés de contenu

pour des partenaires internationaux, disposant de plus de 43 million d'utilisateurs de solutions de sécurité de données dans plus de 100 pays et plus de 1,500,000 appels de clients reçus annuellement pour des services CRM.

Chapitre 3. BitDefender 9 Standard

BitDefender 9 Standard est un excellent produit antivirus, spécialement conçu pour inclure les options spécifiques aux demandes de sécurité des utilisateurs individuels. Sa facilité d'emploi et la mise à jour automatique font de BitDefender 9 Standard un produit antivirus de type "installez et oubliez-le".

3.1. Antivirus

La mission du module Antivirus est d'assurer la détection et la suppression de tous les virus en circulation. L'Antivirus BitDefender utilise des moteurs d'analyse robustes, certifié par ICSA Labs, Virus Bulletin, Checkmark, CheckVir et TÜV.

Heuristic in Virtual Environment. Heuristic in Virtual Environment (HiVE) émule un ordinateur virtuel dans un ordinateur où des morceaux de logiciel sont lancé de manière à vérifier leur comportement potentiellement malveillant. Cette technologie propriétaire de BitDefender représente un nouveau modèle de sécurité qui permet de conserver son système d'exploitation à l'abri de virus inconnus en détectant les morceaux de code malicieux pour lesquels des signatures n'ont pas encore été créées.

Protection Antivirus et Antispyware Permanente. Les nouveaux moteurs d'analyse améliorés de BitDefender analyseront et désinfecteront les fichiers à l'accès, réduisant les pertes de données. Les documents infectés peuvent maintenant être récupérés au lieu d'être effacés.

Protection des Applications Peer-2-Peer. Filtre contre les virus se propageant via les messageries instantanées et les logiciels de partage de fichiers.

Analyse et désinfection des Spywares. BitDefender peut analyser votre système ou une partie de celui-ci, contre les menaces de spywares connus. L'analyse utilise une base de données de signatures de spywares mise à jour constamment.

Protection totale des E-mail. BitDefender vérifie les protocoles POP3/SMTP, filtrant les messages entrants et sortants, quel que soit le client mail utilisé (MS Outlook, MS Outlook Express, Netscape, Eudora, Pegasus, The Bat, etc.), sans aucun besoin de configuration additionnelle.

3.2. Autres Fonctions

Mise à jour chaque heure. Votre version de BitDefender sera mise à jour 24 fois pas jour par Internet, directement ou via un serveur Proxy. Le logiciel est capable de se réparer lui-même si nécessaire, en téléchargeant les fichiers endommagés ou manquants depuis les serveurs de BitDefender. Le possesseur de la licence BitDefender bénéficie de mise à jour gratuite des définitions des virus et des mises à jour logicielles.

Support 24/7. Assuré en ligne par des représentants qualifiés et aussi une base de donnée en ligne répondant aux questions les plus fréquemment posées.

Chapitre 4. Modules BitDefender

BitDefender 9 Standard est composé de modules différents: **Général**, **Antivirus** et **Mise à jour**.

4.1. Module Général

BitDefender est par défaut paramétré pour une sécurité optimale. Les informations essentielles sur les modules de BitDefender sont affichées dans le module Général.

Ici vous pouvez enregistrer votre produit et paramétrer le fonctionnement de BitDefender.

4.2. Module Antivirus

BitDefender vous protège des virus entrant sur votre système en analysant les fichiers, e-mails, téléchargement et tous les autres contenu qui arrivent sur votre ordinateur. Vous accès à tous les paramètres et fonctions de BitDefender depuis ce modules.

La protection Virus est divisée en deux catégories :

- Analyse à l'accès - empêche les nouveaux virus de pénétrer votre système. C'est ce qu'on appelle un bouclier antivirus – les fichiers sont analysés lorsque l'utilisateur y accède. BitDefender analysera par exemple un document Word que vous ouvrez, et les e-mails lors de leur réception. BitDefender analyse les fichiers que vous utilisez.

- Analyse à la demande - détecte les virus qui résident déjà dans votre ordinateur. C'est l'analyse classique antivirus déclanchée par l'utilisateur – vous choisissez le lecteur, dossier ou fichier que BitDefender doit analyser et BitDefender le fait – a la demande.

4.3. Module de mise à jour

De nouveaux virus sont trouvés et identifiés chaque jour. C'est pourquoi il est très important de garder BitDefender à jour avec les dernières signatures de virus. Par défaut, BitDefender recherche automatiquement des mises à jour toutes les heures.

Les mises à jour se déclinent en les parties suivantes:

- **Mise à jour des moteurs antivirus** - comme de nouvelles menaces apparaissent, les fichiers contenant les signatures de virus doivent être mis à jour en permanence contre elles. Elles s'affichent sous le nom de **Virus Definitions Update**.

- **Mise à jour produit** - lorsqu'une nouvelle version du produit est prête, de nouvelles fonctions et techniques d'analyse sont introduites afin d'augmenter les performances du produit. Ces mises à jour sont affichées sous le nom de **Product Update**.

De plus, du point de vue de l'intervention de l'utilisateur, nous proposons :

- **Mise à jour automatique** - l'antivirus contacte automatiquement les serveurs BitDefender afin de vérifier si une mise à jour est disponible. Si c'est le cas, BitDefender est actualisé automatiquement. La mis à jour automatique peut aussi être faite n'importe quand en cliquant **Mise à jour** du module des mises à jour.
- **Mise à jour manuelle** - vous devez télécharger et installer les dernières signatures de virus manuellement.

Console de management

Chapitre 5. Vue d'ensemble

BitDefender 9 Standard a été conçu avec une console de management (gestion) centralisée, qui permet la configuration des options de protection de chaque module BitDefender. Autrement dit, il suffit d'ouvrir la console pour accéder aux différents modules: **Antivirus** et **Mise à jour**.

L'accès à cette console se fait par le menu Démarrer de Windows, en suivant le chemin suivant: **Démarrer** -> **Programmes** -> **BitDefender 9** -> **BitDefender 9 Standard** ou plus rapidement en double-cliquant sur **l'icône BitDefender** dans la zone de notification (en bas à droite à côté de l'horloge).

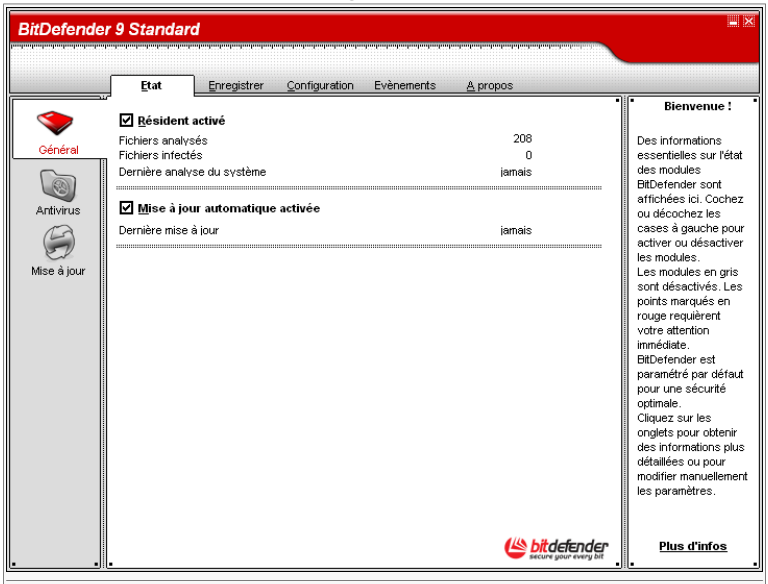

Figure 5.1. Console de management

Sur la partie gauche de la console, vous pouvez sélectionner les modules suivants:

- Général - pour accéder à la section résumant les principaux paramétrages de Bit-Defender, des informations produits et contacts. Vous pouvez également enregistrer le produit à cet endroit.
- Antivirus - pour accéder à la fenêtre de configuration de l'**Antivirus**.
- Mise à jour - pour accéder à la fenêtre de configuration des **Mises à jour**.

Dans la partie droite de la console de gestion vous pouvez voir l'info concernant la section où vous vous trouvez. L'option **Plus d'infos**, placée en bas à droite ouvre la section **Aide**.

5.1. Zone de notification

Lorsque la console est réduite, une icône apparaît dans le zone de notification:

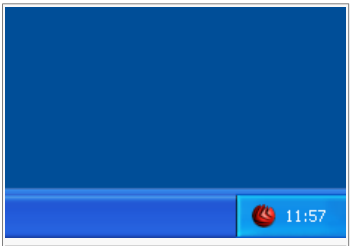

Figure 5.2. Zone de notification

Si vous double-cliquez sur cette icône, la console s'ouvre.

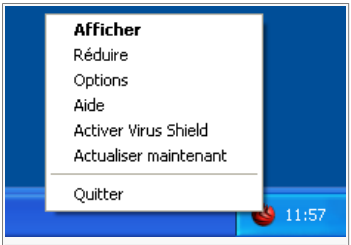

Figure 5.3. Menu Contextuel

De plus, en faisant un clic-droit dessus, un menu contenant les options suivantes, apparaîtra.

- **Afficher** - ouvre la console de contrôle.
- **Réduire** - minimise la console, si elle est ouverte.
- **Options** - ouvre la section Configuration de la console.
- **Aide** - ouvre la documentation électronique.
- **Activer/Désactiver Virus Shield** - active/désactive la protection à l'accès.

- **Actualiser maintenant** - réalise une mise à jour immédiate.
- **Quitter** - ferme l'application. En choisissant cette option, l'icône dans la zone de notification disparaîtra et pour la faire apparaître de nouveau, vous devrez la lancer depuis le menu Démarrer.

Note

- Si vous désactivez une ou plusieurs des modules BitDefender, l'icône sera grisée. Ainsi vous saurez si quelques modules sont désactivés sans ouvrir la console de gestion.
- L'icône va clignoter si une mise à jour est disponible.

5.2. Barre d'analyse d'activité

La **Barre d'analyse d'activité** est une visualisation graphique de l'analyse d'activité de votre système.

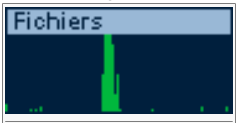

Figure 5.4. Zone fichiers

Les barres vertes (la **Zone de fichiers**) montrent le nombre de fichiers analysés par seconde, sur une échelle de 0 à 50.

Note

La **Barre de l'activité d'analyse** vous annonce si le Résident est désactivé avec une croix rouge sur l'aire correspondante (**Zone Fichier**). Ainsi vous saurez si vous êtes protégé sans ouvrir la console de gestion.

Si vous ne souhaitez plus voir cette barre, il vous suffit de faire un clic-droit dessus et de choisir **Cacher**.

Note

Pour cacher complètement cette fenêtre, décochez l'option **Activer la barre d'activité**(depuis le module **Général**, section Configuration).

Chapitre 6. Module Général

La section **Général** de ce Manuel d'utilisation contient les thèmes suivants:

- Informations Générales
- Enregistrement du Produit
- Paramètres de la console de management
- Evénements
- A propos

6.1. Informations Générales

Pour accéder à cette section, cliquez sur l'onglet **Etat** dans le module **Général**.

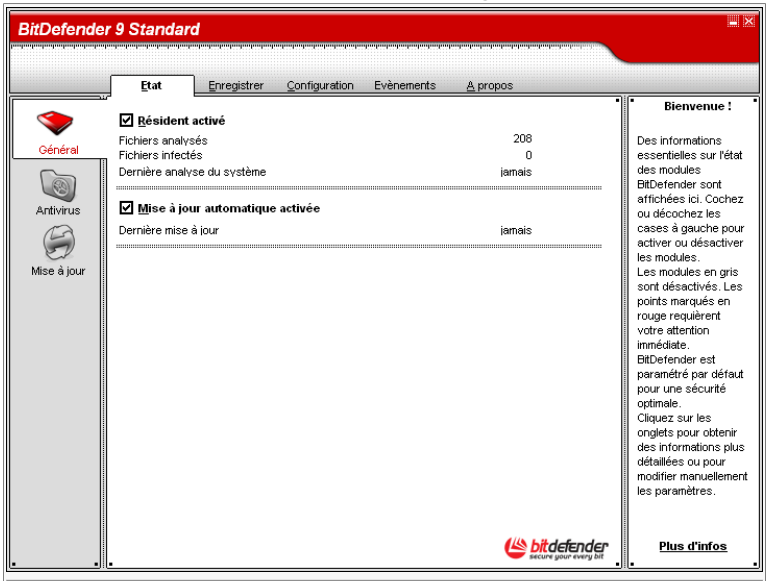

Figure 6.1. Informations Générales

Vous pouvez consulter ici les informations concernant les status du produit.

Pour activer ou désactiver certaines des principales fonctions de BitDefender cocher ou décocher les cases correspondantes.

Avertissement
Les points marqués en rouge nécessitent votre attention immédiate.

6.1.1. Résident

Il fournit une protection permanente en temps réel contre les virus et autres menaces. Cette rubrique affiche le nombre de fichiers analysés, le nombre de fichiers infectés, ainsi que la date de la dernière analyse du système.

Note
Pour prévenir l'infection de votre ordinateur par des virus, laissez le **Résident** activé.

Avertissement
Nous vous recommandons fortement d'analyser complètement au moins une fois par semaine votre système. Pour cela, accédez au **module Antivirus**, section Analyse, cochez **Disques Locaux** puis cliquez sur **Analyse**.

6.1.2. Mise à jour automatique

De nouveaux virus sont identifiés chaque jour. C'est pourquoi il est très important de garder BitDefender à jour avec les dernières signatures de virus. Cette rubrique affiche la date de dernière mise à jour.

Note
Pour protéger vos données critiques, BitDefender peut réaliser des mises à jour automatiques. Laissez l'option **Mise à jour Automatique** activé.

6.2. Enregistrement du Produit

Pour accéder à cette section, cliquez sur l'onglet **Enregistrer** dans le module **Général**.

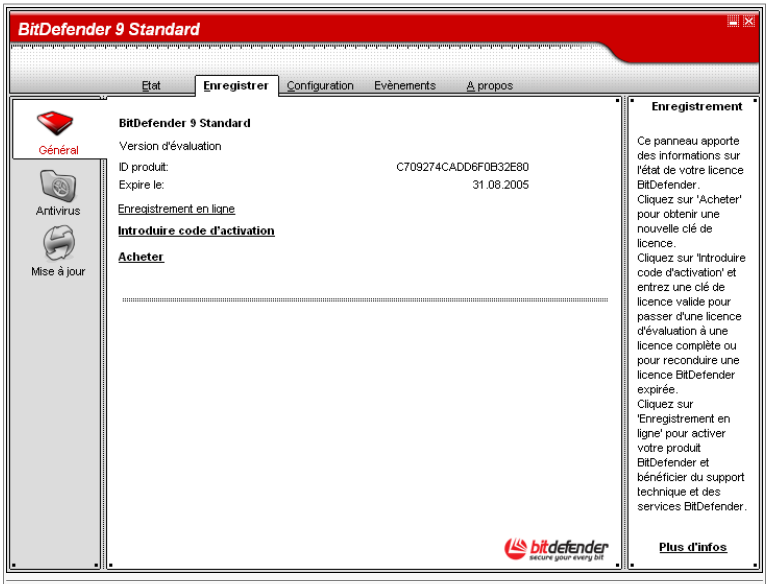

Figure 6.2. Enregistrement du Produit

Cette section contient des informations sur le statut de vos licences BitDefender. Vous pouvez ici enregistrer votre produit et voir sa date d'expiration.

Le produit est livré par défaut avec un code d'évaluation valable 30 jours. A la fin de cette période d'essai, si vous souhaitez acheter le produit (dans le cas où votre version n'est pas un produit complet déjà acheté), vous pouvez cliquer sur le bouton **Acheter** ou vous rendre chez l'un de nos revendeurs.

Clicquez sur **Enregistrement en ligne** pour activer votre produit BitDefender afin de bénéficier du support technique gratuit et des autres services BitDefender.

Pour modifier la licence par défaut, cliquez sur **Introduir code d'activation**. La fenêtre suivante apparaîtra:

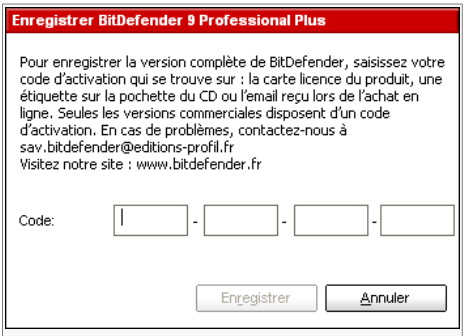

Figure 6.3. Introduire code d'activation

Saisissez votre code dans le champ **Code**. Cliquez sur **Enregistrer** pour finir l'enregistrement.

Si vous faîtes une erreur de saisie, il vous sera demandé de la re-rentrer.

Si vous entrez un code d'activation valide, une boîte de dialogue vous le confirmera.

Dans la section **Enregistrer**, vous pourrez voir à présent la date d'expiration de votre nouveau code d'activation.

6.3. Paramètres de la console de management

Pour accéder à cette section, cliquez sur l'onglet **Configuration** dans le module **Général**.

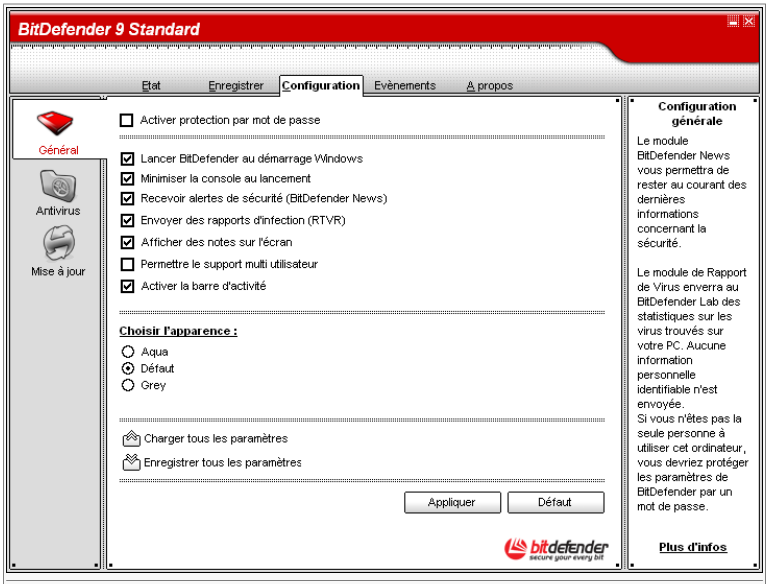

Figure 6.4. Configuration

Vous pouvez dans cette rubrique paramétrer le fonctionnement de BitDefender. Par défaut, BitDefender est chargé au démarrage de Windows et se réduit automatiquement.

Les options suivantes sont disponibles:

- **Activer protection par mot de passe** - permet de choisir un mot de passe afin de protéger la configuration choisie pour BitDefender Management Console configuration;

  Note
  Si vous n'êtes pas le seul utilisateur de votre ordinateur, il est recommandé de protéger vos paramétrages BitDefender par un mot de passe.

  La fenêtre suivante apparaîtra:

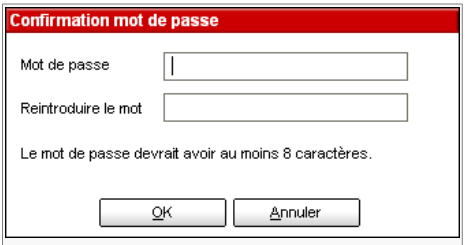

Figure 6.5. Mot de passe

Entrez le mot de passe dans le champ **Mot de passe**, re-saisissez le dans le champ **Reintroduire le mot** de passe et cliquez sur **OK**.

Important
A présent, si vous souhaitez changer les options de configuration de BitDefender, le mot de passe vous sera demandé.

- **Lancer BitDefender au démarrage Windows** - lance automatiquement BitDefender au démarrage du système.

  Note
  Cela est fortement recommandé!

- **Minimiser la console au lancement** - réduit la console de management BitDefender après son chargement au démarrage. Seul l'icône BitDefender apparaîtra dans la zone de notification.
- **Recevoir alertes de sécurité** - affiche régulièrement des informations de sécurité sur des risques de virus et/ou de failles, envoyées par serveurs de BitDefender.
- **Afficher l'écran d'accueil** - montre l'écran qui apparaît lorsque vous lancez Bit-Defender.
- **Envoyer des rapports d'infection** - envoie au laboratoire BitDefender des rapports concernant les virus identifiés sur vote PC. Les informations envoyées contiendront seulement le nom des virus et seront utilisées pour créer des rapports statistiques.

  Le rapport ne contiendra aucune donnée confidentielle, comme votre nom, votre adresse IP ou autre et ne sera pas utilisé à des fins commerciales. Les informations envoyées contiendront seulement le nom des virus et seront utilisées pour créer des rapports statistiques.

- **Afficher des notes sur l'écran** - affiche des fenêtres d'alertes sur les statuts de votre produit.
- **Permettre le support multi utilisateur** - permet aux autres utilisateurs du même ordinateur de garder leur configuration pour BitDefender.

Note

Cet option peut être activée ou pas par les utilisateurs ayant des droits d'administrateur sur la machine locale.

- **Activer la barre d'activité** - active / désactive le « *Barre d'analyse d'activité* » (p. 39).
- **Choisir l'apparence** - permet de sélectionner la couleur de la console de management. Le skin représente l'image de fond de l'interface. Pour sélectionner un skin différent, cliquez sur la couleur correspondante.

Utilisez les boutons **Enregistrer tous les paramètres** / **Charger tous les paramètres** pour sauvegarder ou charger les paramètres établis pour BitDefender dans un endroit spécifié. Ainsi, vous pouvez utiliser les mêmes paramètres après la réinstallation ou la réparation de votre BitDefender.

Cliquez sur **Appliquer** pour enregistrer les modifications. Si vous cliquez sur **Défaut** vous allez charger les paramètres par défaut.

6.4. Evénements

Pour accéder à cette section, cliquez sur l'onglet **Evénements** dans le module **Général**.

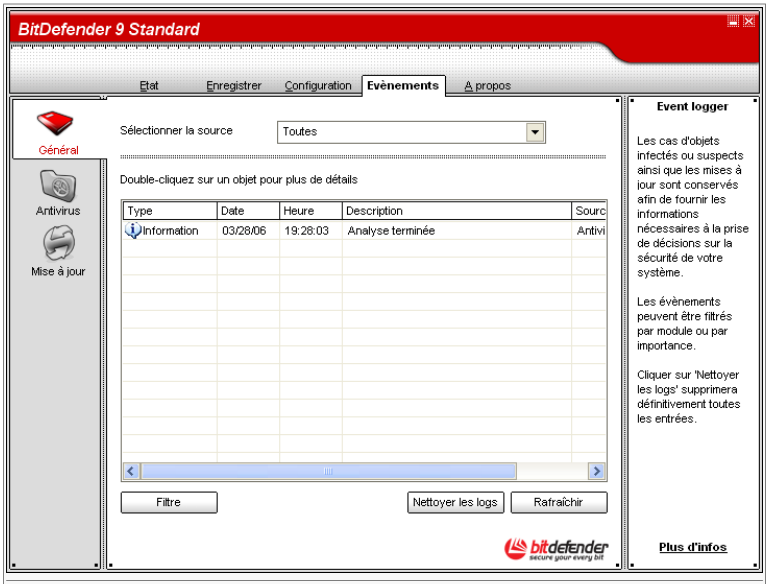

Figure 6.6. Evénements

Toutes les alertes générées par BitDefender sont affichées dans cette section.

Il existe 3 types d'événements: **Information**, **Attention** et **Critique**.

Exemples d'événements:

- **Information** - quand un email est scanné;
- **Attention** - quand un fichier suspect est détecté;
- **Critique** - quand un fichier infecté est détecté.

Pour chaque événement on fournit l'information suivante: la date et le temps de la production de l'événement, une brève description et sa source (**Antivirus** ou **Mise-à-Jour**). Double-cliquez sur un événement pour voir ses propriétés.

Vous pouvez filtrez ces événements de 2 manières (par type ou par source):

- Cliquez **Filtre** pour sélecter les types d'événement à montrer;
- Sélectez la source de l'événement depuis le menu déroulant.

Si la console de gestion est ouverte à la section **d'Evénements** et qu'un même temps un événement apparaît, vous devez cliquer **Rafraîchir** pour voir l'événement.

Pour effacer tous les événements de la liste cliquez **Nettoyer les logs**.

6.5. A propos

Pour accéder à cette section, cliquez sur l'onglet **A propos** dans le module **Général**.

Figure 6.7. A propos

Dans cette section vous pouvez trouver des informations sur votre produit et les contacts dont vous pourriez avoir besoin.

BitDefenderTM fournit des solutions de sécurité pour satisfaire les besoins de protection des environnements informatiques actuels et protège actuellement plus de 120 millions d'utilisateurs particuliers ou professionnels dans plus de 100 pays.

BitDefenderTM est certifié par tous les principaux organismes de tests indépendants - **ICSA Labs**, **CheckMark** et **Virus Bulletin**, et est la seule solution de sécurité à avoir reçu le prix européen de l'innovation technologique **IST Prize**.

Chapitre 7. Module Antivirus

La section **Antivirus** de ce Manuel d'utilisation contient les thèmes suivants:

- Analyse immédiate
- Analyse à la demande
- Analyse programmée
- Quarantaine
- Rapport

7.1. Analyse à l'accès

Pour accéder à cette section cliquez sur l'onglet **Résident** dans le module **Antivirus**.

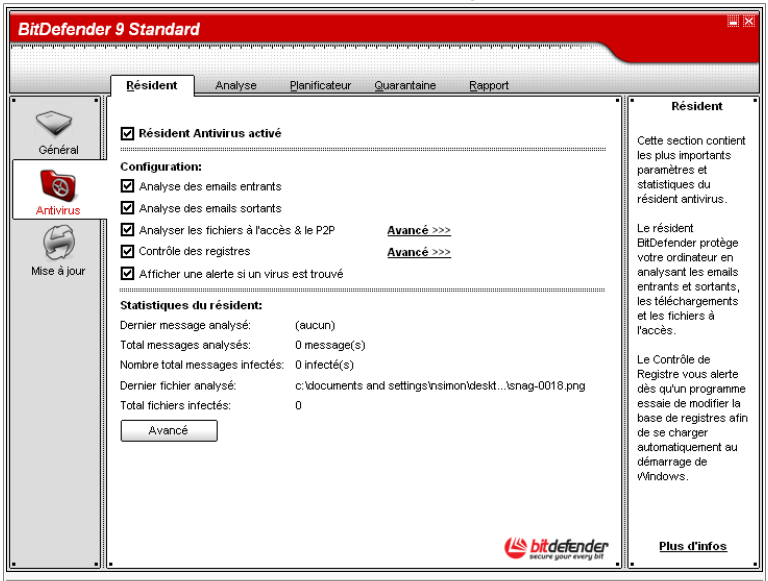

Figure 7.1. Résident

Dans cette section vous pouvez configurer **l'Résident** et vous pouvez voir les informations concernant ses activités. Le **Résident** protège votre ordinateur en analysant les emails, téléchargements et tous les fichiers à l'accès.

Note

Pour prévenir l'infection de votre ordinateur par des virus, garder le **Résident** activé.

En bas de cette section, vous pouvez voir les statistiques de **Résident** sur les fichiers et emails. Cliquez sur **Avancé** si vous voulez une fenêtre plus détaillée au sujet de ces statistiques.

7.1.1. Contrôle des registres

Une partie très importante du système d'exploitation Windows est appelée la **Base de registres**. C'est l'endroit où Windows conserve ses paramétrages, programmes installés, informations sur l'utilisateur et autres.

La **Base de registres** est également utilisée pour définir quels programmes devraient être lancés automatiquement lorsque Windows démarre. Cela est souvent utilisé par les virus afin d'être automatiquement lancé lorsque l'utilisateur redémarre son ordinateur.

Le **Contrôle des registres** garde un oeil sur les registres Windows – c'est également utile pour détecter des chevaux de Troie. Il vous alertera dès qu'un programme essaiera de modifier une entrée dans la base de registres afin de s'exécuter au démarrage de Windows.

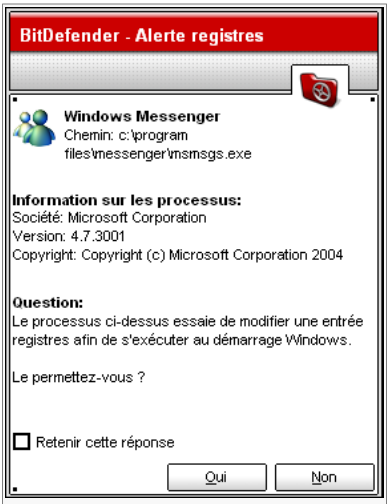

Figure 7.2. Alerte registres

Vous pouvez refuser cette modification en cliquant sur **Non** ou l'autoriser en cliquant sur **Oui**.

Si vous souhaitez que BitDefender se souvienne de votre réponse, cochez la case: **Retenir cette réponse**.

Note
Vos réponses seront la base de la liste de règles.

Si vous souhaitez voir la liste des entrées dans la base de registres, cliquez sur **Avancé>>>** dans **Contrôle des registres**.

Figure 7.3. Contrôle d'accès aux registres

Pour chaque application, un menu extensible sera créé; il contient toutes les modifications des registres.

Pour supprimer une entrée dans les registres, sélectionnez la et cliquez sur **Effacer**. Pour désactiver temporairement une entrée sans la supprimer, décochez la case correspondante.

Note
BitDefender vous alertera à l'installation de nouveaux logiciels nécessitant d'être lancé après le prochain démarrage de votre ordinateur. Dans la plupart des cas, ces programmes sont légitimes et peuvent être autorisés.

7.1.2. Principaux paramétrages

Pour choisir une option, cliquez avec la souris sur la case correspondante.

- **Analyse des emails entrants** - tous les emails entrants seront analysés par BitDefender.
- **Analyse des emails sortants** - tous les emails sortants seront analysés par BitDefender.
- **Analyser les fichiers à l'accès & le P2P** - tous les fichiers à l'accès sont analysés.
- **Afficher une alerte si un virus est trouvé** - une fenêtre d'alerte sera affichée lors de la rencontre d'un virus dans un fichier ou message e-mail.

  Pour un fichier infecté, la fenêtre d'alerte va contenir le nom du virus, le chemin, l'action effectuée par BitDefender et un lien vers le site BitDefender où on peut trouver plus d'informations sur celui-ci. Pour un message e-mail infecté, la fenêtre d'alerte va contenir aussi l'information sur l'expéditeur et le destinataire.

  Au cas où un fichier suspect est détecté vous pouvez lancer un assistant à partir de la fenêtre d'alerte qui vous aidera envoyer ce fichier au Laboratoire BitDefender

pour une analyse ultérieure. Vous pouvez saisir votre adresse email pour recevoir des informations sur ce rapport.

7.1.3. D'autres options

Les utilisateurs avancés peuvent vouloir tirer profit des paramètres d'analyse proposé par BitDefender. L'analyseur peut être paramétré pour exclure certains types d'extensions, de répertoire ou d'archives que vous savez inoffensifs. Cliquez sur **Avancé>>>** dans **Analyser les fichiers à l'accès & le P2P** pour explorer ces paramètres .

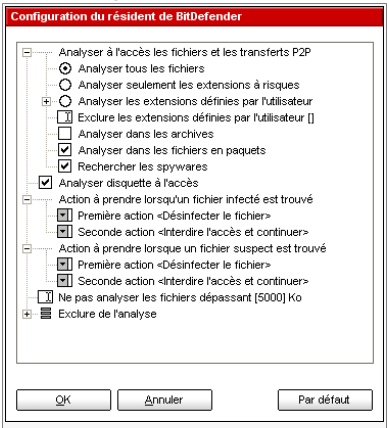

Figure 7.4. Configuration du résident

Cliquez la case avec "+" pour ouvrir une option ou la case avec "-" pour fermer une option. Vous pouvez observer que certaines options d'analyse, bien que le signe "+" apparaisse, ne peuvent s'ouvrir. La raison est que ces options n'ont pas encore été sélectionnées. Vous observerez que si vous les cochez, elles pourront être ouvertes.

- Sélectionner **Analyser à l'accès les fichiers et les transferts P2P** - pour analyser les fichiers à l'accès ainsi que les communications et échanges Peer To Peer (messageries instantanées comme ICQ, NetMeeting, Yahoo! Messenger, MSN Messenger – logiciels de téléchargement comme Kazaa, Emule, Shareaza). Après cela, sélectionnez le type de fichiers que vous voulez analyser.

  Les options suivantes sont disponibles:

Option	Description
Analyse de tous les fichiers	Tous les fichiers à l'accès seront analysés, quelque soit leur type.
Analyse seulement les extensions à risques	Seuls les fichiers avec les extensions suivantes seront analysés : `.exe`; `.bat`; `.com`;

Option	Description
	.dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml et .nws.
Analyse les extensions définies par l'utilisateur	Seuls les fichiers avec les extensions définies par l'utilisateur seront analysés. Ces extensions doivent être séparées par ";".
Exclure les extensions définies par l'utilisateur	Tous les fichiers à l'accès seront analysés à l'exception de ceux avec des extensions définies par l'utilisateur. Ces extensions doivent être séparées par ";".
Analyser dans les archives	Les archives serons également analysées. Avec cette option activée, l'ordinateur sera ralentit.
Analyser dans les fichiers en paquets	Tous les fichiers en paquets seront analysés.
Rechercher les spywares.	Recherche les applications spyware. Ces fichiers sont traités comme des fichiers infectés. Les logiciels contenant des composants de type adware peuvent ne plus fonctionner si cette option est activée.

- Sélectionnez **Analyse disquette à l'accès** - si vous souhaitez analyser les disquettes à l'accès.
- Cliquez sur la rubrique **Action quand un virus est trouvé** - et sélectionnez dans la liste la première action sur les fichiers infectés. BitDefender permet de sélectionner deux actions dans le cas où un fichier infecté est trouvé.

  Vous pouvez sélectionner l'une des actions suivantes:

Action	Description
Interdire l'accès et continuer	Dans le cas où un fichier infecté est détecté, l'accès à celui-ci est interdit.
Désinfecter le fichier	Pour désinfecter un fichier infecté.
Effacer le fichier	Supprimer un fichier infecté, sans alerte.
Déplacer en quarantaine	Les fichiers infectés sont déplacés en quarantaine.

- Cliquez sur la rubrique **Deuxième action quand la première échoue** - et sélectionnez dans la liste la seconde action sur les fichiers infectés.

  Les options suivantes sont disponibles:

Action	Description
Interdire l'accès et continuer	Dans le cas où un fichier infecté est détecté, l'accès à celui-ci est interdit.
Effacer le fichier	Supprimer un fichier infecté, sans alerte.
Déplacer en quarantaine	Les fichiers infectés sont déplacés en quarantaine.

  Il est possible de définir des actions différentes pour les fichiers infectés et pour les fichiers détectés comme suspects..

- **Ne pas analyser les fichiers dépassant à** - tapez la taille maximum des fichiers à analyser. Si vous mettez la taille à 0, tous les fichiers seront analysés.

- **Exclure de l'analyse** - cliquez sur "+" afin de spécifier un répertoire qui sera exclu de l'analyse. La conséquence sera d'ajouter une nouvelle option, `Nouveau choix`. Cliquez sur la boîte correspondante à ce nouveau choix et à partir de la fenêtre d'exploration, sélectionnez le répertoire que vous souhaitez exclure de l'analyse.

Cliquez sur **OK** pour enregistrer les modifications ou cliquez sur **Par Défaut** pour charger les paramètres par défaut.

7.2. Analyse à la demande

Pour accéder à cette section cliquez sur l'onglet **Analyse** dans le module **Antivirus**.

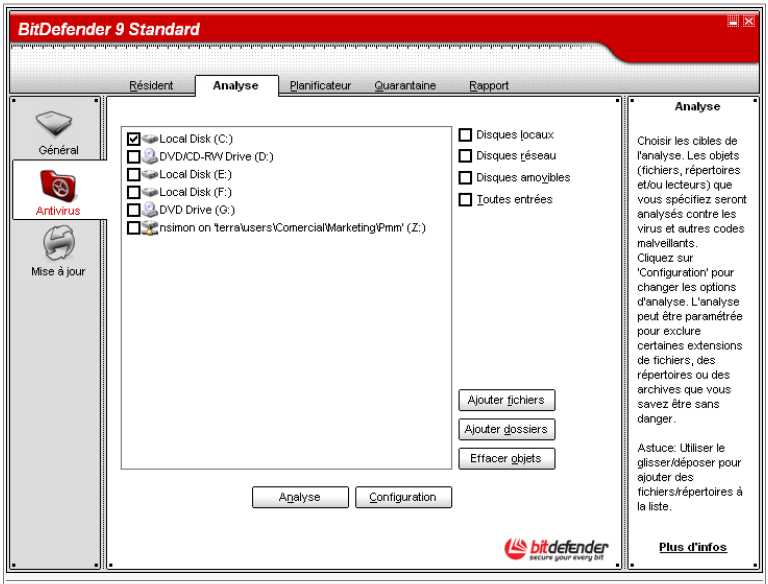

Figure 7.5. Analyse

Dans cette section vous pouvez configurer BitDefender pour analyser votre ordinateur.

L'objectif principal de BitDefender est de conserver votre PC sans virus. Cela est assuré avant tout par l'analyse antivirus des emails que vous recevez et des fichiers que vous téléchargez ou copiez sur votre système.

Il y a cependant un risque qu'un virus soit déjà logé dans votre système, avant même l'installation de BitDefender. C'est pourquoi il est prudent d'analyser votre ordinateur après l'installation de BitDefender. Et c'est encore plus prudent d'analyser régulièrement votre ordinateur contre les virus.

BitDefender permet quatre types d'analyse à la demande:

- Analyse immediate - il y a quelques étapes à suivre pour analyser votre ordinateur contre les virus;
- Analyse contextuelle - un clic-droit sur un fichier ou répertoire permet de sélectionner Analyse avec BitDefender;
- Analyse par glisser-déplacer - glissez & déplacez un fichier ou un répertoire sur la barre d'analyse d'activité;

- Analyse programmée - vous pouvez programmer BitDefender pour analyser votre système contre les virus périodiquement.

7.2.1. Analyse immédiate

Pour analyser votre ordinateur contre les virus, veuillez suivre les étapes suivantes:

Etape 1/5 - Fermez tous les programmes ouverts

Afin de permettre à BitDefender de réaliser une analyse complète, il est nécessaire de fermer tous les programmes ouverts, tout spécialement les clients de messagerie (ex : Outlook, Outlook Express ou Eudora).

Etape 2/5 - Vérifiez que BitDefender est à jour contre les derniers virus

Avant de laisser BitDefender analyser votre ordinateur, vous devriez vérifier que BitDefender est à jour de ses signatures de virus, dans la mesure où de nouveaux virus apparaissent chaque jour. Vous pouvez vérifier de quand date la dernière mise à jour en bas du module Mise à jour.

Etape 3/5 - Choisissez la cible de l'analyse

Dans la console de management, entrez dans le module **Antivirus** et cliquez sur l'onglet Analyse. Par défaut, la section contient une image de la structure des partitions du système. A côté de cela, des boutons et options d'analyse peuvent également être observés.

Cette section contient les boutons suivants:

- **Ajouter fichiers** - ouvre une fenêtre de navigation dans laquelle vous pouvez choisir le fichier.
- **Ajouter dossiers** - ouvre une fenêtre de navigation dans laquelle vous pouvez choisir le dossier.

Note
Vous pouvez rajouter des fichiers et des dossiers à la liste d'analyse en les glissant-déposant.

- **Effacer sélection** - efface le fichier/dossier sélectionné auparavant.

Note
Seulement les fichiers/dossiers rajoutés après peuvent être effacés, mais pas ceux qui sont automatiquement "proposés" par BitDefender.

- **Configuration** - ouvre une fenêtre dans laquelle vous pouvez spécifier quels types de fichiers sont à analyser, l'action sur les fichiers infectés, la génération de messages d'alertes, la sauvegarde des résultats d'analyse dans des fichiers rapports.
- **Analyse** - lance l'analyse en tenant compte des options choisies.

Ces options permettent une sélection rapide des cibles d'analyses.

- **Disques locaux** - pour analyser les disques locaux.
- **Disques réseaux** - pour analyser tous les lecteurs réseaux.
- **Disques amovibles** - pour analyser les disques amovibles (CD-ROM, lecteur de disquettes).
- **Toutes entrées** - pour analyser l'ensemble des lecteurs, peu importe qu'ils soient locaux, réseaux ou amovibles.

Note
Si vous voulez analyser l'ensemble de votre ordinateur, cochez la case **Toutes entrées**.

Important
Si vous n'êtes pas habitué à paramétrer, vous pouvez à présent cliquer sur le bouton **Analyse**. BitDefender commencera l'analyse de votre PC avec les paramétrages standard, qui sont suffisants.

Etape 4/5 - Sélectionnez les options d'analyse

Les utilisateurs avancés peuvent vouloir tirer avantage des possibilités de paramétrage d'analyse de BitDefender. Le scanner peut être paramétré pour éviter certaines extensions de fichiers, répertoires ou archives que vous savez être sans danger. Cela peut considérablement réduire le temps d'analyse et améliorer le temps de réaction de votre ordinateur durant une analyse.

Cliquer sur **Configuration** dans la section Analyse pour explorer ces options .

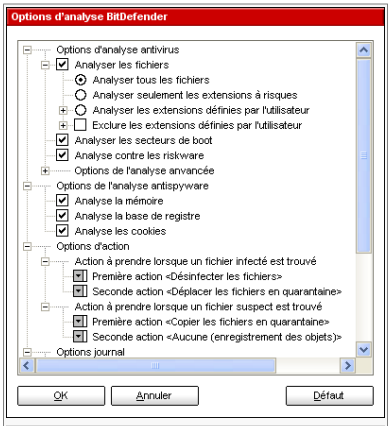

Figure 7.6. Options d'analyse

Les options d'analyse sont organisés en menus extensibles très proche de ceux qui sont utilisés dans l'explorateur Windows.

Les options d'analyse sont groupées en cinq catégories:

- **Options d'analyse antivirus**
- **Options de l'analyse antispyware**
- **Options d'action**
- **Options jurnal**
- **Autres options**

Note
Cliquez sur la case avec un "+" pour ouvrir une option et sur la case avec un "-" pour fermer une option.

- Spécifiez le type d'objets à analyser (archives, e-mail et autres) et d'autres options. Cela est réalisé par la sélection de certaines options dans la catégorie **Options d'analyse antivirus**.

  Les options suivantes sont disponibles:

Option	Description
Analyser les fichiers	**Analyser tous les fichiers** Pour analyser tous les fichiers, quelque soit leur type.

Option		Description
	Analyser seulement les extensions à risques	Pour analyser seulement les fichiers avec les extensions suivantes: exe; bat; com; dll; ocx; scr; bin; dat; 386; vxd; sys; wdm; cla; class; ovl; ole; exe; hlp; doc; dot; xls; ppt; wbk; wiz; pot; ppa; xla; xlt; vbs; vbe; mdb; rtf; htm; hta; html; xml; xtp; php; asp; js; shs; chm; lnk; pif; prc; url; smm; pdf; msi; ini; csc; cmd; bas; eml et nws.
	Analyser les extensions définies par l'utilisateur	Pour analyser seulement les fichiers avec les extensions définies par l'utilisateur. Ces extensions doivent être séparées par ";".
	Exclure les extensions définies par l'utilisateur	Pour analyser tous les fichiers, à l'exception de ceux avec des extensions définies par l'utilisateur. Ces extensions doivent être séparées par ";".
Analyser les secteurs de boot		Pour analyser les secteurs de boot du système.
Analyse contre les riskware		Analyse contre des menaces autres que virales, tels que les dialers et adwares. Ces fichiers sont traités comme des fichiers infectés. Les logiciels contenant des composants de type adware peuvent ne plus fonctionner si cette option est activée.
Options de l'analyse avancée	**Ouvrir les paquets programmes**	Analyser les fichiers en paquets.
	Ouvrir les archives	Analyser l'intérieur des archives.
	Ouvrir les archives de messagerie	Analyser dans les archives de messagerie.
	Utiliser la détection heuristique	Active l'analyse heuristique des fichiers. Le but de l'analyse heuristique est d'identifier de nouveaux virus, se basant sur des algorithmes spécifiques, avant que ces virus soient connus. De fausses alertes peuvent apparaître et cette méthode ne peut pas garantir un taux de détection à 100% de ces nouveaux virus.

Option	Description
	Quand un tel fichier est détecté il est classifié comme étant suspect. Dans ce cas, nous vous recommandons d'envoyer le fichier au laboratoire BitDefender afin qu'il soit analysé.
Détecter les corps de virus incomplets	Détecte les corps de virus incomplets.

- Spécifiez la cible d'analyse antispyware (processus, cookies et mémoire). Cela est réalisé par la sélection de certaines options dans la catégorie **Options de l'analyse antispyware**.

  Les options suivantes sont disponibles:

Option	Description
Analyse la memoire	Recherche les spywares dans les processus.
Analyse la base de registre	Analyse les entrées du Régistre.
Analyse les cookies	Analyse les fichiers cookies.

- Spécifier l'action à appliquer aux fichiers suspects et infectés. Ouvre **Options d'action** pour voir toutes les actions possibles sur les fichiers infectés.

Action	Description
Aucune (enregistrement des objects)	Pour rapporter la détection d'un fichier infecté et le nom du virus.
Demander l'action à l'utilisateur	Quand un fichier infecté est détecté, une fenêtre apparaît, demandant à l'utilisateur de choisir une action à appliquer au fichier. Suivant l'importance du fichier, vous pouvez choisir de le désinfecter, l'isoler en quarantaine ou l'effacer.
Désinfecter les fichiers	Pour désinfecter les fichiers infectés.
Supprimer les fichiers	Pour effacer les fichiers infectés.

Action	Description
Renommer les fichiers	Pour renommer les fichiers infectés. La nouvelle extension des fichiers infectés sera `.vir`. En renommant les fichiers infectés, la possibilité d'exécuter et donc de propager l'infection disparaît. En même temps, ils peuvent être sauvegardés pour un examen et analyse ultérieur.
Copier les fichiers en quarantaine	Pour copier les fichiers infectés dans la zone de quarantaine. Cela revient concrètement à dupliquer le fichier infecté dans la zone de quarantaine, mais le fichier infecté ne sera pas retiré de son emplacement d'origine.
Déplacer les fichiers en quarantaine	Déplacer les fichiers infectés dans la zone de quarantaine.

- L'étape suivante permet de sélectionner les options du rapport. Pour faire cela, vous devrez cocher le signe "+" correspondant aux **Options de rapport**. Ces options permettent la création d'un fichier rapport (fichier qui contient des informations au sujet du processus d'analyse).

Option		Description
Afficher tous les fichiers analysés		Affiche tous les fichiers, infectés ou pas, et leur état dans un fichier journal. Avec cette option activée, l'ordinateur sera ralenti.
Créer un fichier journal	**Nom du fichier rapport**`vscan.log`	Ceci est un champ qui permet le changement du nom du fichier rapport. Cliquez sur cette option et introduire un nouveau nom.
	Ajouter au rapport existant	Ajoute les informations sur la dernière analyse à la fin du journal, après celles déjà existantes.
	Limiter la taille du journal à [x] Ko	Cliquez sur cette option et introduisez la taille maximum du fichier dans le champ qui apparaît.

Note
Vous pouvez voir le fichier de rapport dans la section Rapport du module **Antivirus**.

- Ouvrir la catégorie **Autres Options** depuis laquelle vous pourrez sélectionner les options suivantes.

Option	Description
Exécuter la tâche d'analyse avec une priorité basse	Décroît la priorité du processus d'analyse. Vous allez permettre aux autres logiciels d'être exécutés à une vitesse supérieure et d'augmenter le temps nécessaire pour le final du processus d'analyse.
Arrêter le PC lorsque l'analyse est terminée	Eteindre le PC à la fin de l'analyse.
Soumettre les fichiers suspects au BitDefender Lab	Il vous sera demandé de soumettre les fichiers suspects aux laboratoires BitDefender à la fin de l'analyse.
Réduire la fenêtre d'analyse au démarrage dans la zone de notification	Réduit la fenêtre d'analyse dans la zone de notification. Double-cliquez sur l'icône de BitDefender pour l'ouvrir.
Demander pour le redémarrage	Si l'action nécessite un redémarrage, demander à l'utilisateur.

Cliquez sur **OK** pour enregistrer les modifications ou cliquez sur **Défaut** pour charger les paramètres par défaut.

Etape 5/5 - Analyse virale

Une fois les options d'analyse choisies, tout ce qu'il vous reste à faire est de démarrer l'analyse. Pour le faire, cliquez sur **Analyse**. La fenêtre d'analyse apparaîtra:

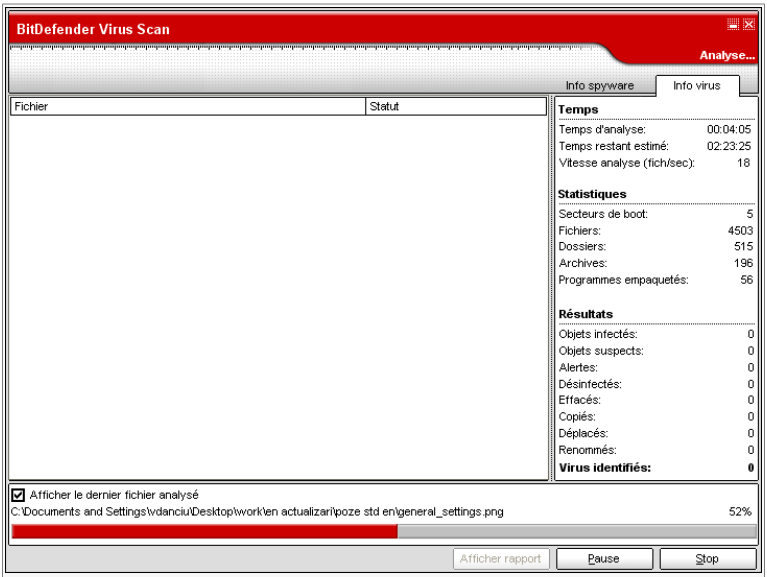

Figure 7.7. Virus Scan

Pendant l'analyse, BitDefender affiche la progression de l'analyse et vous alerte en cas de détection de menaces. Dans la partie droite, vous pouvez voir les statistiques de l'analyse en cours. Selon le choix d'analyse, des informations sur les spywares et/ou les virus sont disponibles. Si les deux sont disponibles, cliquez sur l'onglet correspondant pour en savoir plus sur l'analyse des virus ou des spywares.

Cochez la case correspondante à **Afficher le dernier fichier analysé** et seulement les informations sur les derniers fichiers analysés seront visibles.

Note
L'analyse peut durer un certain temps, suivant la taille de votre disque.

Si vous cliquez:

- **Stop** - une nouvelle fenêtre s'affichera vous permettant de stopper la vérification du système.
- **Pause** - l'analyse s'arrête temporairement – vous pouvez la continuer en cliquant sur **Continuer**.

- **Afficher rapport** - le rapport d'analyse s'ouvre.

Note
Le fichier rapport est sauvegardé automatiquement dans la section Rapport du module **Antivirus**.

Une icône apparaîtra dans le Systray quand le processus d'analyse se déroule.

7.2.2. Analyse contextuelle

Faîtes un clic-droit sur le fichier ou répertoire que vous souhaitez analyser et sélectionnez l'option **BitDefender Antivirus v9**.

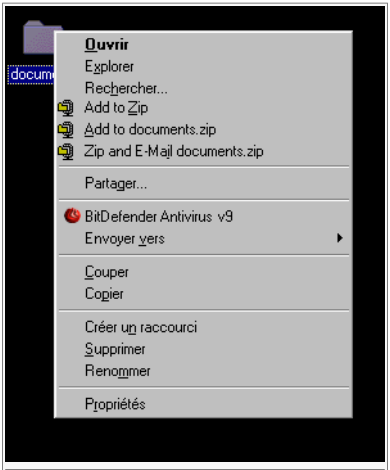

Figure 7.8. Analyse contextuelle

Un fichier rapport nommé `vscan.log` sera créé et accessible dans le module **Antivirus**, section Rapport .

7.2.3. Analyse par glisser & déposer

Glissez le fichier ou répertoire que vous voulez analyser et déposez le sur la **Barre d'analyse d'Activité**, comme sur l'image ci-dessous.

Figure 7.9. Glisser le fichier

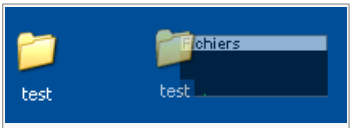

Figure 7.10. Déposer le fichier

Un fichier rapport nommé `activbar.log` sera créé et accessible dans le module **Antivirus**, section Rapport .

Dans les deux cas (analyse contextuelle et analyse par glisser & déposer) la fenêtre d'analyse apparaîtra. Si un virus est détecté, une fenêtre d'alerte apparaîtra.

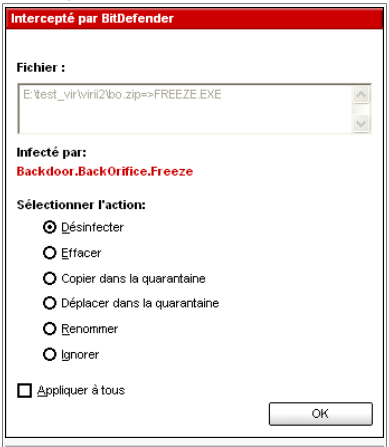

Figure 7.11. Mode d'action

Vous pouvez voir le nom du fichier et le nom du virus. Vous pouvez sélectionner une des options suivantes:

- **Désinfecter** - désinfecter le fichier infecté;
- **Effacer** - effacer le fichier infecté;
- **Copier dans la quarantaine** - copier le fichier infecté dans la zone de quarantaine;
- **Déplacer dans la quarantaine** - déplacer le fichier infecté dans la zone de quarantaine;
- **Renommer** - pour renommer le fichier infecté. La nouvelle extension des fichiers infectés sera `.vir`.
- **Ignorer** - ignorer l'infection. Aucune action ne sera appliquée au fichier infecté.

Si vous analysez un répertoire, et que vous souhaitez que l'action sur les fichiers infectés soit la même pour tous, cochez l'option **Appliquer à tous**.

Note

Si l'option **Désinfecter** n'est pas activée, cela veut dire que le fichier ne peut pas être désinfecter. Le meilleur choix est alors de l'isoler en quarantaine et de nous l'envoyer, ou de le supprimer.

Cliquez sur **OK**.

7.2.4. Analyse programmée

Pour accéder à cette section cliquez sur l'onglet **Planificateur** dans le module **Antivirus**.

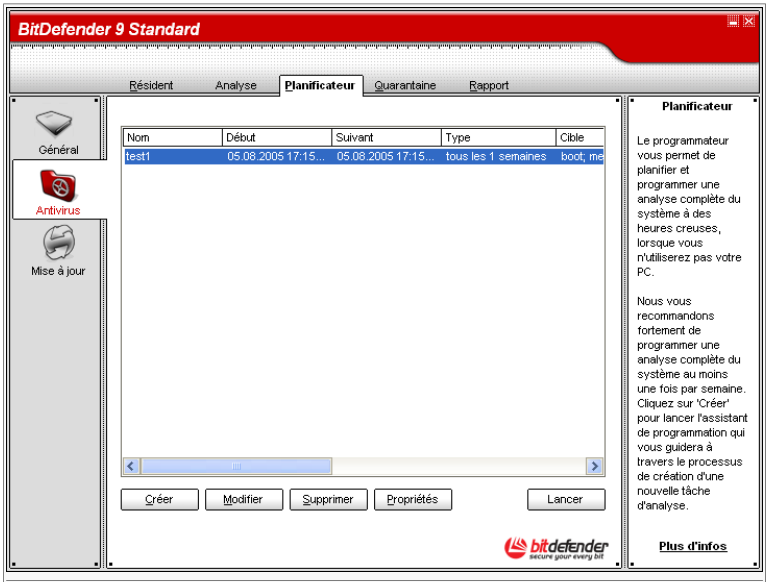

Figure 7.12. Antivirus Planificateur

Etant donné que l'analyse prendra du temps, et qu'elle fonctionnera mieux si vous avez fermé les autres programmes, il est préférable pour vous de programmer une analyse à une heure où vous n'utilisez pas votre ordinateur. Cela implique que l'utilisateur doit à l'avance créer une tâche.

Le **Planificateur** intègre un assistant de création de nouvelles tâches d'analyse. Il vous assistera chaque fois que vous aurez besoin de faire une opération sur ces

évènements, que ce soit pour créer une nouvelle tâche ou pour en modifier une existante.

Le **Planificateur** contient quelques boutons pour administrer les tâches d'analyse.

- **Creér** - lance l'assistant qui vous guidera dans la création d'une nouvelle tâche d'analyse.
- **Modifier** - modifie les propriétés d'une tâche précédemment créée. Cela lance également l'assistant.

> **Note**
> Si vous modifiez le nom d'un évènement, un nouvel évènement sera créé, sous le nouveau nom saisi.

- **Supprimer** - efface une tâche sélectionnée.
- **Lancer** - démarre immédiatement la tâche choisie.
- **Propriétés** - affiche les propriétés d'une tâche sélectionnée.

L'écran du Planificateur contient également une liste où toutes les tâches peuvent être vues, avec leur nom, la date de première exécution, la date de la prochaine exécution et son type (périodique ou une fois seulement).

Si vous faites un clic-droit sur une tâche programmée, un menu s'affichera comme celui ci-dessous.

> **Note**
> Le **Planificateur** permet un nombre illimité de tâches d'analyse.

Vous pouvez également naviguer à travers les tâches d'analyse en utilisant le clavier: appuyer sur la touche **Supprimer** pour effacer une tâche, pressez la touche **Entrée** afin de voir les propriétés de l'événement sélectionné ou appuyez sur la touche **Inser** pour créer une nouvelle tâche (l'assistant du Planificateur se lancera).

> **Note**
> Utilisez les touches de navigation pour faire défiler la page de bas en haut et de gauche à droite.

Cliquez sur **Creér**. Cela lancera l'assistant de création de tâches.

Etape 1/9 - Intro

Figure 7.13. Intro

Tapez le nom du nouvel évènement dans le champ **Nom tâche** et un court descriptif dans le champ **Description tâche**.

Les options suivantes sont disponibles:

- **Exécuter la tâche en priorité basse** - Baisse la priorité de la tâche d'analyse. Cela permettra à d'autres programmes de fonctionner plus rapidement mais augmentera le temps nécessaire pour finir l'analyse.
- **Réduire la fenêtre d'analyse** - Réduit la fenêtre d'analyse dans la zone de notification. Double-cliquez sur l'icône de BitDefender pour l'ouvrir.
- **Arrêter le PC une fois l'analyse terminée** - Arrêter le PC à la fin de l'analyse.

Cliquez sur **Suivant** pour continuer. Si vous cliquez sur **Annuler** une fenêtre apparaîtra pour vous demander confirmation.

Etape 2/9 - Date et heure dèbut

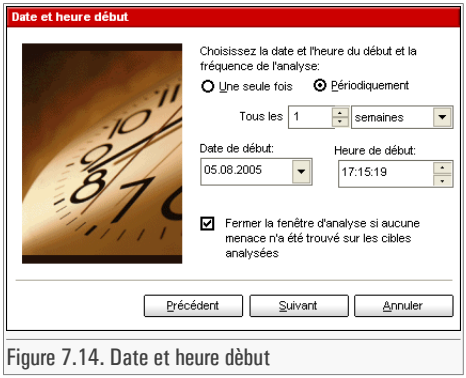

Figure 7.14. Date et heure dèbut

Suite à cela, une fenêtre où vous pourrez sélectionner le type d'analyse s'affichera.

- Cochez la case **Une seule fois** si vous voulez programmer une analyse ponctuelle.
- Si vous souhaitez que l'analyse soit répétée après un certain intervalle, cochez la case **Périodiquement**.

Sélectionnez l'intervalle - minutes, heures, jours, semaines, mois, années – après lequel l'analyse sera répétée.

Important
Si vous choisissez une analyse répétée, l'évènement sera lancé pour une période de temps illimitée. Afin de le stopper, il doit être effacé de la liste des évènements de la fenêtre du Planificateur.

Si vous voulez fermer automatiquement la fenêtre d'analyse si des fichiers infectés ou suspects n'ont pas été trouvés pendant le processus d'analyse, sélectez la case à cocher correspondant à cette option.

Cliquez sur **Précédent** pour revenir en arrière ou cliquez sur **Suivant** pour continuer.

Etape 3/9 - Cible

Figure 7.15. Cible

Vous pouvez sélectionner les objets suivants: Le choix de l'analyse est divisé en deux catégories:

- **Analyse contre les virus** - recherche les virus.

Note
Sélectionner la case correspondante pour activer l'analyse des virus.

Les options suivantes sont disponibles:

Option		Description
Boot		Analyse le secteur de boot, afin d'identifier les virus de boot.
Fichiers		Analyse les fichiers.
	Mail	Analyse les archives de mail.
	Archives	Analyse à l'intérieur des archives.
	Fichiers en paquets	Analyse les fichiers en paquets.
	Riskware	Analyse contre des menaces autres que virales, tels que les dialers et adwares. Ces fichiers sont traités comme des fichiers infectés.

- **Analyse contre les spywares** - recherche les applications spyware.

Note
Sélectionner la case correspondante pour activer l'analyse des spywares.

Les options suivantes sont disponibles:

Option	Description
Cookies	Analyse les cookies.
Régistres	Analyse les entrées du Régistre.
Mémoire	Analyse la mémoire.

Pour activer/désactiver un choix de recherche, cochez ou décochez la case correspondante.

Cliquez sur **Précédent** pour revenir en arrière ou cliquez sur **Suivant** pour continuer.

Etape 4/9 - Chemin cible

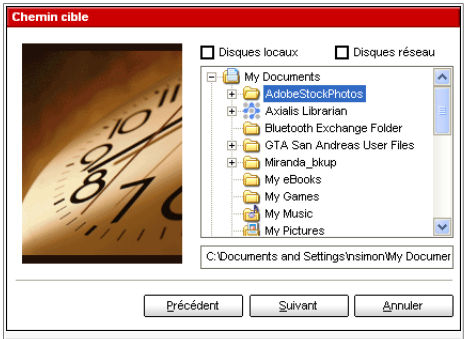

Figure 7.16.

Ici vous devez spécifier le répertoire des objets à analyser. Cette étape est nécessaire si vous avez sélectionné l'analyse de fichiers dans l'étape précédente.

Cet écran est une fenêtre d'exploration qui vous permet de sélectionner les partitions et répertoires à analyser. Lorsque le curseur est placé sur un répertoire, le chemin complet du répertoire apparaîtra dans le champ inférieur.

Note
Cliquez sur la case “+" pour ouvrir une option ou sur celle "-" pour fermer une option.

Par ailleurs, pour sélectionner les éléments à analyser, vous pouvez utiliser les options de sélection rapide placées en haut de la fenêtre:

- **Disques locaux** - pour analyser tous les disques locaux;
- **Disques réseau** - pour analyser tous les disques du réseau.

Cliquez sur **Précédent** pour revenir en arrière ou cliquez sur **Suivant** pour continuer.

Etape 5/9 - Type de fichiers

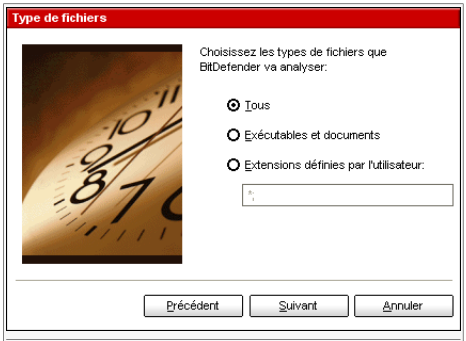

Figure 7.17. Type de fichiers

Spécifiez les types e fichiers à analyser. Cette étape est nécessaire si vous avez sélectionné l’analyse de fichiers dans l’étape précédente.

Cet écran est une fenêtre d’exploration qui vous permet de sélectionner les partitions et répertoires à analyser. Lorsque le curseur est placé sur un répertoire, le chemin complet du répertoire apparaîtra dans le champ inférieur.

Vous pouvez sélectionner:

- **Tous** - pour analyser tous les fichiers, quel que soit leur type;
- **Exécutables et documents** - pour analyser les fichiers programmes et les documents;

- **Extensions définies par l'utilisateur** - pour analyser seulement les fichiers dont l'extension apparaît dans la liste.

Important
Ces extensions doivent être séparées par ";".

Cliquez sur **Précédent** pour revenir en arrière ou cliquez sur **Suivant** pour continuer.

Etape 6/9 - Type d'analyse

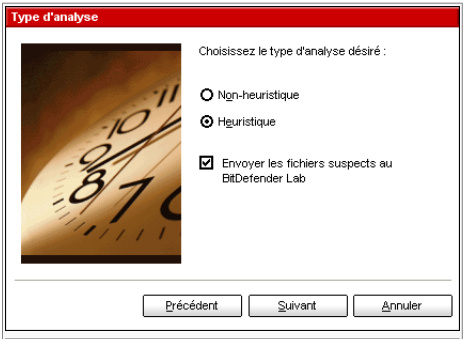

Figure 7.18. Type d'analyse

Sélectionnez le type d'analyse:

- **Non-heuristique** - analyse les fichiers avec une procédure basée sur des signatures de virus connus;
- **Heuristique** - représente une méthode basée sur certains algorithmes, qui permettent d'identifier de nouveaux virus encore inconnus. Parfois, elle peut générer des rapports de codes suspects dans des programmes normaux, ce que l'on appelle des "false positive" (ou fausse alerte).

Vous disposez du choix suivant:

- **Envoyer les fichiers suspects au BitDefender Lab** - Il vous sera demandé de soumettre les fichiers suspects aux laboratoires BitDefender à la fin de l'analyse.

Cliquez sur **Précédent** pour revenir en arrière ou cliquez sur **Suivant** pour continuer.

Etape 7/9 - Mode d'action

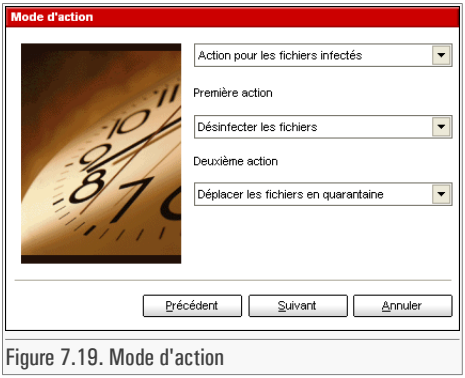

Figure 7.19. Mode d'action

BitDefender permet de choisir deux actions dans le cas où des fichiers infectés sont trouvés. Vous pouvez sélectionner l'une des actions suivantes.

Action	Description
Aucune (enregistrement des objects)	Aucune action ne sera prise sur les fichiers infectés. Ceux-ci vont apparaître dans le fichier des rapports.
Demander l'action à l'utilisateur	Chaque fois qu'un fichier infecté est détecté, une boîte de dialogue est affichée, dans laquelle l'utilisateur peut sélectionner l'action à entreprendre sur ce fichier. Suivant l'importance du fichier, vous pouvez choisir de le désinfecter, l'isoler en quarantaine ou l'effacer.
Désinfecter les fichiers	Pour désinfecter les fichiers infectés.
Supprimer les fichiers	Pour supprimer les fichiers infectés.
Renommer les fichiers	Pour changer l'extension des fichiers infectés. La nouvelle extension des fichiers infectés sera `.vir`. En renommant les fichiers infectés, la possibilité d'exécuter et donc de propager l'infection disparaît. En même temps, ils peuvent être sauvegardés pour un examen et analyse ultérieur.

Action	Description
Copier les fichiers en quarantaine	Pour copier les fichiers infectés dans la zone de quarantaine. Cela revient concrètement à dupliquer le fichier infecté dans la zone de quarantaine, mais le fichier infecté ne sera pas retiré de son emplacement d'origine.
Déplacer les fichiers en quarantaine	Les fichiers infectés sont déplacés en quarantaine. Lorsque le virus est en quarantaine il ne peut avoir aucune action néfaste.

Note
Nous vous recommandons de sélectionner **Désinfecter** en première action et **Déplacer en Quarantaine** en seconde action.

Il est possible de définir des actions différentes pour les fichiers infectés et pour les fichiers détectés comme suspects.

Cliquez sur **Précédent** pour revenir en arrière ou cliquez sur **Suivant** pour continuer.

Etape 8/9 - Info rapport

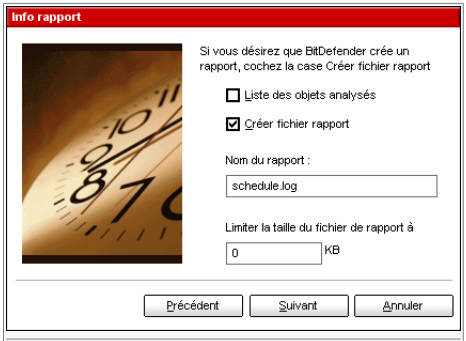

Figure 7.20. Info rapport

Pour créer un rapport d'analyse, cliquez sur **Créer fichier rapport**. Dès lors, les autres options pour la création d'un fichier rapport seront activées.

Tapez le nom du fichier rapport dans la case **Nom du rapport**. Par défaut, le nom est `schedule.log`. Il contiendra toutes les informations concernant le processus d'analyse : le nombre de virus identifiés, le nombre de fichiers analysés, le nombre de fichiers désinfectés et supprimés.

Vous pouvez également limiter la taille du fichier des rapports. Introduisez la taille maximum du fichier dans le champs correspondant.

Si vous souhaitez voir les informations sur l'ensemble des fichiers scannés, infectés ou non, sélectionnez l'option **Liste des fichiers analysés**. Une fois l'option cochée, l'ordinateur sera ralenti.

Note
Vous pouvez voir le fichier rapport dans la section Rapport du module **Antivirus**.

Cliquez sur **Précédent** pour revenir en arrière ou cliquez sur **Suivant** pour continuer.

Etape 9/9 - Récapitulatif

Figure 7.21. Récapitulatif

Il s'agit de la dernière étape dans la création d'une tâche d'analyse. Dans cette fenêtre vous pouvez, voir tous les paramétrages de la tâche d'analyse et vous pouvez les modifier en retournant sur les étapes précédentes (**Précédent**).

Si vous ne souhaitez faire aucune modifications, cliquez sur **Terminer**.

La nouvelle tâche apparaîtra dans la section Planificateur.

7.3. Quarantaine

Pour accéder à cette section cliquez sur l'onglet **Quarantaine** dans le module **Antivirus**.

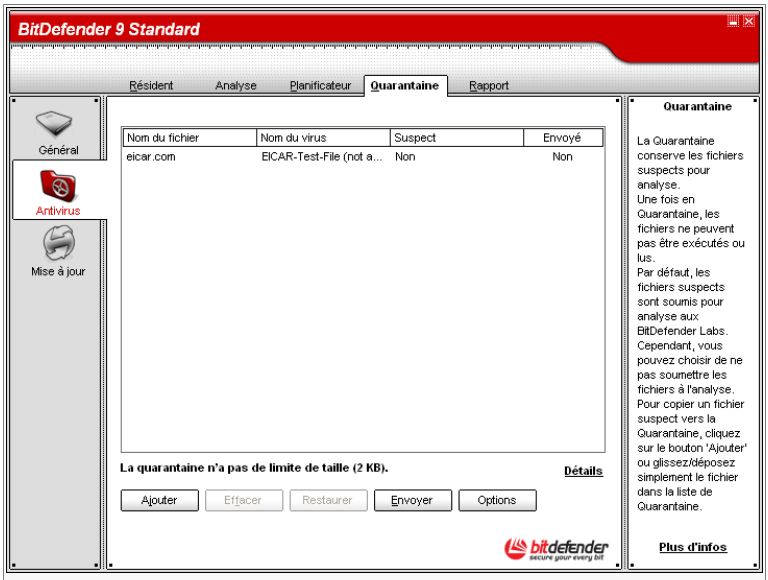

Figure 7.22. Quarantaine

BitDefender permet d'isoler les fichiers infectés ou suspects dans une zone sécurisée, nommée quarantaine. En isolant ces fichiers dans la quarantaine, le risque d'être infecté disparaît et, en même temps, vous avez la possibilité d'envoyer ces fichiers pour une analyse par le VirusLab de BitDefender.

La section qui permet d'administrer ces fichiers isolés est la **Quarantaine**. Ce module a été conçu avec une fonction d'envoi automatique des fichiers infectés au VirusLab.

Comme vous le constaterez, la section **Quarantaine** contient une liste de tous les fichiers qui ont été isolés jusque là. Chaque fichier intègre son nom, sa taille, sa date d'isolation et sa date de soumission. Si vous voulez voir plus d'informations à propos des fichiers en quarantaine, cliquez sur **Plus d'infos**.

Note
Lorsque le virus est en quarantaine, il ne peut faire aucun dégât puisqu'il ne peut être exécuté ou lu.

La section **Quarantaine** contient des boutons pour administrer ces fichiers.

- **Ajouter** - ajoute des fichiers à la quarantaine. Utilisez ce bouton pour mettre en quarantaine un fichier que vous soupçonner d'être infecté. Une fenêtre s'ouvrira et vous pourrez sélectionner le fichier depuis son emplacement sur le disque. De cette façon, le fichier est copié en quarantaine.

  Si vous voulez déplacer le fichier en zone de quarantaine, vous devez cocher la case **Supprimer de l'emplacement d'origine**. Une méthode plus rapide d'ajouter des fichiers suspects à la quarantaine est de les glisser & déposer dans la liste de quarantaine.

- **Effacer** - efface les fichiers sélectionnés de votre ordinateur;

- **Restaurer** - remet le fichier sélectionner à son emplacement d'origine.

- **Envoyer** - envoie les fichiers sélectionnés pour analyse au VirusLab.

  Important
  Vous devez spécifier quelques informations pour pouvoir les soumettre. Pour cela, cliquez sur **Paramétrages** et complétez les champs de la section **Configuration de la proposition**, comme décrit ci-dessous.

- **Options** - ouvre les options avancées pour la zone de quarantaine. La fenêtre suivante s'ouvrira:

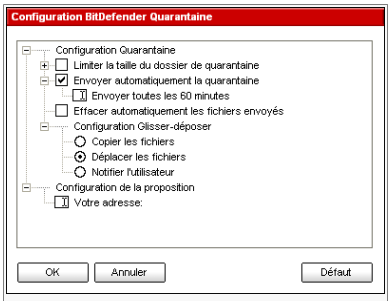

Figure 7.23. Configuration Quarantaine

Les options de quarantaine sont groupées en deux catégories:

- **Configuration Quarantaine**
- **Configuration de la proposition**

Note

Cliquez sur la case avec un "+" pour ouvrir une option ou la boîte avec un "-" pour fermer une option.

Configuration Quarantaine

- **Limiter la taille du dossier de quarantaine** - maintient sous contrôle la taille de la quarantaine. Cette option est activée par défaut et sa taille est de 12 000 kbs. Si vous voulez changer cette valeur, vous pouvez en introduire une autre dans le champ. Si vous choisissez l'option **Effacer automatiquement les vieux fichiers**, les fichiers les plus anciens seront automatiquement supprimés du fichier de quarantaine pour libérer de la place pour les nouveaux fichiers.
- **Envoyer automatiquement la quarantaine** - envoie automatiquement les fichiers en quarantaine au VirusLab pour analyse. Vous pouvez paramétrer le délai entre deux envois consécutifs dans le champs **Envoyer toutes les x minutes**.
- **Effacer automatiquement les fichiers envoyés** - supprime automatiquement les fichiers en quarantaine après les avoir envoyés au VirusLab pour analyse.
- **Configuration Glisser & Déposer** - si vous utilisez la méthode du glisser & déposer pour ajouter de nouveaux fichiers à la quarantaine, vous pouvez ici spécifier l'action : copier, déplacer ou demander à l'utilisateur.

Configuration de la proposition

- **Votre adresse** - entrez votre adresse e-mail dans le cas où vous souhaitez recevoir une réponse de nos experts au sujet des fichiers suspects soumis pour analyse.

Cliquez sur **OK** pour enregistrer les modifications ou cliquez sur **Défaut** pour charger les paramètres par défaut.

7.4. Rapport

Pour accéder à cette section cliquez sur l'onglet **Rapport** dans le module **Antivirus**.

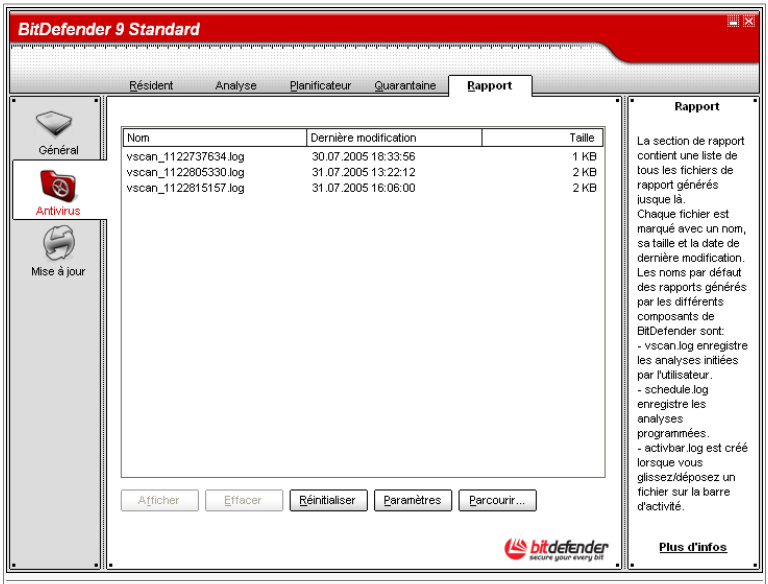

Figure 7.24. Rapport

La section **Rapport** contient une liste de tous les fichiers rapports générés. Chaque fichier a son nom, sa taille et sa date de dernière modification.

Lors du lancement d'un processus d'analyse, l'utilisateur a la possibilité d'opter pour la création d'un fichier rapport où il peut voir des informations au sujet de l'analyse. L'utilisateur peut voir ces rapports depuis la console de management.

BitDefender conservera des traces de sa propre activité sur votre ordinateur. Les fichiers rapports par défaut sont les suivants:

- Vscan.log est créé lorsque vous scannez immédiatement votre système;
- Schedule.log vient des tâches d'analyse que vous pouvez avoir paramétré;
- Activbar.log est créé lorsque vous analysez par la fonction glisser &déposer.

La section **Rapport** contient des boutons créés pour l'administration de ces fichiers rapports. La fonction de chacun de ces boutons est expliquée ci-après:

- **Afficher** - ouvre le fichier rapport sélectionné;

- **Effacer** - supprime le fichier rapport sélectionné;
- **Réinitialiser** - réinitialise la section **Rapport**. Si la console de management est ouverte à la section **Rapport** et que vous réalisez dans le même temps une analyse de votre ordinateur, le nouveau fichier rapport avec les résultats d'analyse ne sera visible seulement qu'après avoir cliqué sur **Réinitialiser**.
- **Parcourir** - ouvre une fenêtre dans laquelle vous pouvez sélectionner le fichier rapport que vous souhaitez voir.

Note
Les fichiers rapports sont sauvegardés par défaut dans le répertoire d'installation de BitDefender. Si vous avez sauvegardé les fichiers rapports dans un autre répertoire, vous devez utiliser le bouton **Parcourir** pour les localiser.

- **Paramètres** - permet d'accéder aux options avancées du dossier de rapport. La fenêtre suivante s'ouvrira:

Figure 7.25. Paramètres du rapport

Note
Cliquez sur la case avec un "+" pour ouvrir une option ou la boîte avec un "-" pour fermer une option.

- **Supprimer automatiquement les anciens rapports** - permet de surveiller le nombre de rapports conservés en supprimant ceux dont l'existence dépasse un certain nombre de jours. La durée par défaut est de 180 jours. Vous pouvez modifier cette valeur en la remplaçant par une nouvelle valeur dans la case correspondante.

- **Créer les rapports dans le répertoire** - détermine le dossier dans lequel seront sauvegardés les rapports.

Cliquez sur **OK** pour enregistrer les modifications ou cliquez sur **Défaut** pour charger les paramètres par défaut.

Chapitre 8. Module mise à jour

La section **Mise à jour** de ce Manuel d'utilisation contient les thèmes suivants:

- Mise à jour automatique
- Mise à jour manuelle
- Configuration du Mise à jour

8.1. Mise à jour automatique

Pour accéder à cette section cliquez sur l'onglet **Mise à jour** dans le module **Mise à jour**.

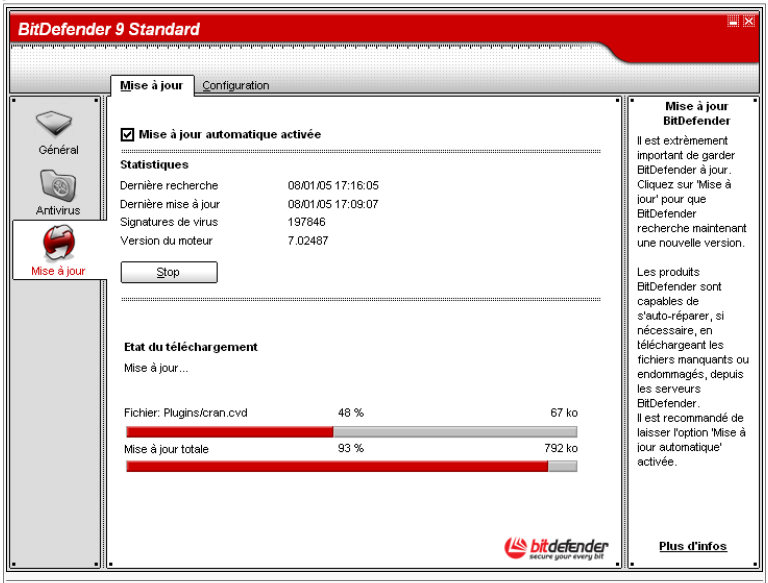

Figure 8.1. Mise à jour

Si vous êtes connecté à Internet par câble ou xDSL, BitDefender se charge de cela lui-même. Il recherche de nouvelles signatures de virus lorsque vous démarrez votre ordinateur et ensuite toutes les heures.

Si une mise-à-jour a été détectée, selon les options paramétrées dans la section Options de mise à jour automatique on vous demandera la confirmation pour la mise-à-jour ou bien la mise-à-jour sera faite automatiquement.

La mis à jour automatique peut aussi etre faite n'importe quand en cliquant sur **Mise à jour**. Cette mis à jour est connu aussi comme **Mise à jour a la demande d'utilisateur**.

Le module **Mise à jour** se connectera au serveur BitDefender et vérifiera la disponibilité d'une mise à jour. Si une mise-à-jour a été détectée, selon les options paramétrées dans la section Paramétres de la mise à jour manuelle, on vous demandera la confirmation pour la mise-à-jour ou bien la mise-à-jour sera faite automatiquement.

Important
Il peut être nécessaire de redémarrer votre PC lorsque vous avez terminé une mise à jour. Nous vous recommandons de le faire dès que possible.

Note
Si vous êtes connecté à Internet par une connexion RTC (ou Numéris), alors c'est une bonne idée que de prendre l'habitude de mettre à jour BitDefender par une demande utilisateur.

8.2. Mise à jour manuelle

Cette méthode permet d'installer les dernières définitions des virus. Pour installer des mises à jour pour la dernière version veuillez utiliser la mise à jour automatique.

Important
Utilisez la mis à jour manuelle quand la mis à jour automatique ne peut pas être effectuée ou quand l'ordinateur n'est pas connecté au Internet.

Il y a 2 moyens pour faire une mis à jour manuelle:

- Avec le fichier `weekly.exe`;
- Avec les `archives zip`.

8.2.1. Mis à jour manuelle avec `weekly.exe`

Le paquet de mis à jour `weekly.exe` est lancé chaque Vendredi et il inclut toutes les signatures des virus et les moteurs antivirus disponible à cette date.

Pour mettre a jour BitDefender en utilisant `weekly.exe`, merci de suivre les pas suivants:

1. Téléchargez weekly.exe et sauvegardez le sur votre disque dur.
2. Localisez le fichier d'installation et double-cliquez dessus avec la souris pour lancer l'assistant de mis à jour.
3. Cliquer **Next**.
4. Cocher **I accept the terms in the License Agreement** et puis **Next**.
5. Cliquer **Install**.
6. Cliquer **Finish**.

8.2.2. Mis à jour manuelle avec des `archives zip`

Il y a deux archives sur le serveur des mises a jour, contenant les mis à jour du moteur antivirus et les définitions des virus: `cumulative.zip` et `daily.zip`.

- `cumulative.zip` est lancé chaque semaine, le Lundi et il inclut toutes les mises a jour des définitions des virus et du moteur antivirus disponible a cette date.
- `daily.zip` est lancé chaque jour et il inclut toutes les mises a jour des définitions des virus et le moteur antivirus depuis le dernier cumulative et jusqu'à cette date.

Bitdefender utilise une architecture basée sur les services. Pour cette raison la procédure pour remplacer les définitions des virus peut être différente pour chaque système d'exploitation:

- Windows NT-SP6, Windows 2000, Windows XP.
- Windows 98, Windows Millennium.

Windows NT-SP6, Windows 2000, Windows XP

Pas a suivre:

1. **Téléchargez la mis à jour appropriée .** S'il est Lundi, merci de télécharger cumulative.zip et de le sauvegarder quelque part sur votre disque dur, quand vous serez interrogé. Sinon, merci de télécharger daily.zip et de le sauvegarder sur votre disque dur. Si c'est la première fois que vous mettez a jour l'antivirus en utilisant la mis à jour manuelle, merci de télécharger tout les deux fichiers.

2. Arrêtez les protections BitDefender

   - **Sortez de la console de management .** Clique droite sur l'icône Bitdefender de la zone de notification et choisissez **Exit**.

   - **Ouvrez les services .** Cliquez sur **Démarrer**, puis **Panneau de configuration**, double-cliquez sur **Outils d'administration** et cliquez sur **Services**.

   - **Arrêtez BitDefender Virus Shield service .** Sélectionnez le service **BitDefender Virus Shield** dans la liste et cliquez sur **Arrêter**.

   - **Arrêtez BitDefender Scan Server service .** Sélectionnez le service **BitDefender Scan Server** dans la liste et cliquez sur **Arrêter**.

3. **Décompressez le contenu de l'archive .** Commencez avec `cumulative.zip` quand tout les deux sont disponibles. Décompressez le contenu dans le dossier `C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\` et acceptez le recouvrage des fichiers existants.

4. Redémarrer BitDefender.

   - **Démarrez le service BitDefender Scan Server .** Sélectionnez le service **BitDefender Scan Server** dans la liste et cliquez sur **Démarrer**.

   - **Démarrez le service BitDefender Virus Shield .** Sélectionnez le service **BitDefender Virus Shield** dans la liste et cliquez sur **Démarrer**.

   - Ouvrez La console de management BitDefender.

Windows 98, Windows Millennium

Pas a suivre:

1. **Téléchargez la mis à jour appropriée .** S'il est Lundi, merci de télécharger cumulative.zip et de le sauvegarder quelque part sur votre disque dur, quand vous serez interrogé. Sinon, merci de télécharger daily.zip et de le sauvegarder sur votre disque dur. Si c'est la première fois que vous mettez a jour l'antivirus en utilisant la mis à jour manuelle, merci de télécharger tout les deux fichiers.

2. **Décompressez le contenu de l'archive .** Commencez avec `cumulative.zip` quand tout les deux sont disponibles. Décompressez le contenu dans le dossier `C:\Program Files\Common Files\Softwin\BitDefender Scan Server\Plugins\` et acceptez le recouvrage des fichiers existants.

3. Redémarrer votre système.

8.3. Configuration du Mise à jour

Pour accéder à cette section cliquez sur l'onglet **Configuration** dans le module **Mise à jour**.

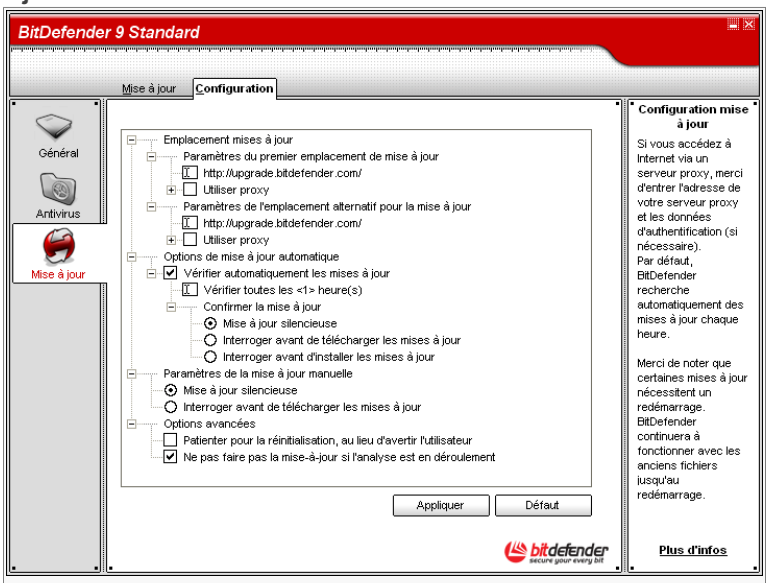

Figure 8.2. Configuration

Les mises à jour peuvent être réalisées depuis le réseau local, depuis Internet, directement ou à travers un serveur proxy.

La fenêtre avec les paramétrages de mises à jour contient 4 catégories d'options (**Emplacement mises à jour**, **Options de mise à jour automatique**, **Paramétres de la mise à jour manuelle** et **Options avancées**) organisées en menus extensibles, similaires à ceux de Windows.

Note

Cliquez sur la case "+" pour ouvrir une option ou sur celle "-" pour fermer une option.

8.3.1. Emplacement mises à jour

Pour des mises à jour plus rapides et plus fiables, vous pouvez établir deux locations de mise à jour: une **Premier emplacement de mise à jour** et une **Emplacement alternatif de mise à jour**. Pour les deux, vous devez établir les options suivantes:

- **Emplacement mises à jour** - Si vous êtes connectés à un réseau local sur lequel sont placées les signatures de virus de BitDefender, vous pouvez changer l'emplacement des mises à jour ici. Par défaut, c'est le suivant: http://upgrade.bitdefender.com.
- **Utilisez proxy** - Dans le cas où la société utilise un serveur proxy, cochez cette option. Les paramétrages suivants doivent être spécifiés:
  - **Serveur proxy** - tapez l'IP ou le nom du serveur proxy et le port que BitDefender doit utiliser pour se connecter au serveur proxy.

    

    Important

    Syntaxe: `nom:port` ou `ip:port`.

  - **Utilisateur** - tapez ici un nom d'utilisateur reconnu par le proxy.

    

    Important

    Syntaxe: `domaine\utilisateur`.

  - **Mot de passe** - tapez ici un mot de passe valide pour l'utilisateur précédemment spécifié.

8.3.2. Options de mise à jour automatique

- **Vérifier automatiquement les mises à jour** - BitDefender contrôle automatiquement nos serveurs pour la disponibilité de mises à jour.
- **Vérifier toutes les x heures** - Paramétrez la fréquence de recherche de mise à jour de BitDefender. L'intervalle de temps par défaut est de 1 heure.
- Il y a trois types de mise à jour automatique:
  - **Mise à jour silencieuse** - BitDefender télécharge et implémente automatiquement la mise à jour.
  - **Interroger avant de télécharger les mises à jour** - chaque fois qu'une mise à jour est disponible, elle vous sera proposée avant d'être téléchargée.
  - **Interroger avant d'installer les mises à jour** - chaque fois qu'une mise à jour a été téléchargée, il vous sera demandé votre accord avant son installation.

Important

Si vous sélectez **Interroger avant de télécharger les mises à jour** ou **Interroger avant d'installer les mises à jour** et si vous fermez et quittez la console de gestion, la mise-à-jour automatique ne sera pas effectuée.

8.3.3. Paramétres de la mise à jour manuelle

- **Mise à jour silencieuse** - BitDefender télécharge et implémente automatiquement la mise à jour.
- **Interroger avant de télécharger les mises à jour** - chaque fois qu'une mise à jour est disponible, elle vous sera proposée avant d'être téléchargée.

Important

Si vous sélectez **Interroger avant de télécharger les mises à jour** et si vous fermez et quittez la console de gestion, la mise-à-jour automatique ne sera pas effectuée.

8.3.4. Options avancées

- **Patienter pour la réinitialisation, au lieu d'avertir l'utilisateur** - Si une mise à jour nécessite la réinitialisation, le produit utilisera les fichiers anciens jusqu'à la réinitialisation du système. L'utilisateur ne sera pas averti sur la réinitialisation, c'est pourquoi le processus de mise à jour de BitDefender ne perturbera pas le travail de l'utilisateur.
- **Ne pas faire la mise-à-jour si l'analyse est en déroulement** - BitDefender ne se mettra pas à jour si une analyse est en cours afin de ne pas perturber ce processus.

Note
Si une mise à jour de BitDefender a lieu pendant l'analyse, celle-ci sera interrompue.

Cliquez sur **Appliquer** pour enregistrer les modifications ou cliquez sur **Défaut** pour charger les paramètres par défaut.

Meilleurs conseils

Chapitre 9. Meilleurs conseils

La section **Meilleurs conseils** de ce Manuel d'utilisation contient le thème suivant:

- Antivirus

9.1. Antivirus

Etapes à suivre pour vous assurer un PC sans virus&spyware:

1. Après la fin de l'installation, enregistrez le produit comme décrit dans la section « *Enregistrement du Produit* » (p. 42).
2. Réalisez une mise à jour de vos signatures de signatures virales « *Mise à jour automatique* » (p. 87).
3. Faites une analyse complète de votre système comme décrit dans la section « *Analyse immédiate* » (p. 59).
4. Dans la section Etat du module **Général** laissez activées les plus importantes options de BitDefender: **Résident** et **Mise à jour automatique**.
5. Programmez BitDefender à analyser votre système au moins une fois par semaine, utilisant l'assistant du « *Analyse programmée* » (p. 69).

Meilleurs conseils

Obtenir de l'aide

Chapitre 10. Support

10.1. Support

Editions Profil et SOFTWIN font le maximum pour apporter à leurs clients une aide rapide et efficace. Les centres de support listés ci-dessous sont continuellement mis à jour avec les nouvelles descriptions de virus et réponses aux questions communes, de manière à ce que vous obteniez les informations nécessaires aussi rapidement que possible.

Nous dédions à nos clients le temps et l'argent qu'ils méritent en accordant le plus haute importance aux nouvelles technologies. De plus, nous pensons qu'un commerce compétitif se base sur une bonne communication et un engagement à l'excellence du support.

Vous êtes libre de demander de l'aide à cette adresse <sav.bitdefender@editions-profil.fr> quand vous le désirez. Pour une réponse rapide, veuillez inclure votre email et autant de détails possible sur votre produit BitDefender, à propos de votre système et essayez de décrire votre problème de manière claire et précise.

10.2. Aide en ligne

10.2.1. Base de connaissances BitDefender

La base de connaissance de BitDefender est un base en ligne d'information concernant les logiciels BitDefender. Elle contient, dans un format facilement accessible, les rapports d'incidents survenus et constatés par le support technique, les équipes de réparation des bugs de BitDefender. Ainsi que des articles généraux sur la prévention antivirus, la gestion des solutions BitDefender, des informations détaillées et beaucoup d'autres articles.

La base de connaissances de BitDefender est ouverte au public et consultable gratuitement. Cet ensemble d'information est une autre manière de fournir aux clients de BitDefender les informations techniques dont ils ont besoin. Toutes les requêtes valides d'information ou les rapports de bug venant de clients de BitDefender trouvent

une réponse en cherchant dans la base de donnés de BitDefender, comme les rapports de bugs, travaux associés, feuillet ou article d'information venant compléter les fichiers d'aide des produits.

La base de connaissance BitDefender est disponible en permanence sur http://kb.bitdefender.com.

10.3. Contact

Une communication efficace est la clé d'une relation réussie. N'hésitez pas à nous contacter concernant les problèmes ou questions que vous pourriez avoir.

10.3.1. Adresses Web

Département des ventes: <commercial@editions-profil.fr>
Support Technique : <sav.bitdefender@editions-profil.fr>
Documentation: <documentation@bitdefender.com>
Programme de Partenariat : <bitdefender@editions-profil.fr>
Marketing: <marketing@editions-profil.fr>
Relations Média : <communication@editions-profil.fr>
Offres d'emplois : <jobs@bitdefender.com>
Soumissions Virus : <virus_submission@bitdefender.com>
Soumissions Spam : <spam_submission@bitdefender.com>
Rapport d'Abus : <abuse@bitdefender.com>
Site web du Produit : http://www.bitdefender.fr
Archives ftp du Produit : ftp://ftp.bitdefender.com/pub
Distributeurs Locaux : http://www.bitdefender.com/partner_list
Base de connaissances BitDefender : http://kb.bitdefender.com

10.3.2. Adresses

Les bureaux de BitDefender se tiennent prêts à répondre à vos questions concernant leur zone d'opération, à propos de questions commerciales et générales. Leur adresse respective et contacts sont listés ci-dessous.

Germany

Softwin GmbH
Karlsdorfer Straße 56 88069
Tettnang

Technischer Support: <support@bitdefender.de>
Vertrieb: <vertrieb@bitdefender.de>
Phone: 07542/94 44 44
Fax: 07542/94 44 99
Product web site: http://www.bitdefender.de

Spain

Constelación Negocial, S.L
C/ Balmes 195, 2ª planta, 08006
Barcelona
Soporte técnico: <soporte@bitdefender-es.com>
Ventas: <comercial@bitdefender-es.com>
Phone: +34 932189615
Fax: +34 932179128
Sitio web del producto: http://www.bitdefender-es.com

U.S.A

BitDefender LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33308
Technical support: <support@bitdefender.us>
Sales: <sales@bitdefender.us>
Phone: 954 776 62 62, 800 388 80 62
Fax: 954 776 64 62, 800 388 80 64
Product web site: http://www.bitdefender.us

Romania

SOFTWIN
5th Fabrica de Glucoza St.
PO BOX 52-93
Bucharest
Technical support: <suport@bitdefender.ro>
Sales: <sales@bitdefender.ro>
Phone: +40 21 2330780
Fax: +40 21 2330763
Product web site: http://www.bitdefender.ro

France

Editions Profil S.A.
49 rue de la Vanne
92120
Montrouge
Support technique: <sav.bitdefender@editions-profil.fr>
Ventes: <commercial@editions-profil.fr>
Téléphone: +33.1.47.35.72.73.
Fax: +33.1.47.35.07.09.
Site web : http://www.bitdefender.fr

Glossaire

ActiveX	ActiveX est un modèle pour écrire des programmes tels que d'autres programmes et le système d'exploitation puissent les appeler. La technologie ActiveX est utilisée par Microsoft Internet Explorer pour faire des pages Web interactives qui ressemblent et se comportent comme des programmes informatiques classiques, plutôt que comme des pages statiques. Avec ActiveX, les utilisateurs peuvent demander ou répondre à des questions, utiliser des boutons et interagir d'autres façons avec les pages Web. Les commandes ActiveX sont souvent écrites en Visual Basic. Active X est reconnu pour un manque total de commandes de sécurité; les experts en sécurité informatique déconseillent son utilisation sur Internet.
Adware	Les adwares sont souvent associés à des applications gratuites ce qui implique leur acceptation par l'utilisateur. Ces adwares étant généralement installés après que l'utilisateur en ait accepté le principe dans un accord de licence, ils ne peuvent pas être considérés comme illégaux. Cependant les « pop up » publicitaires peuvent devenir contrariant et dans certains cas dégrader les performances du système. De plus, les informations collectées peuvent mettre en péril la vie privée des utilisateurs qui ne s'étaient pas complètement rendu compte des termes de l'accord de licence.
Applette Java	Il s'agit d'un programme Java conçu pour s'exécuter seulement dans une page Web. Pour utiliser une applette dans une page Web, vous devez spécifier le nom de l'applette et la taille (la longueur et la largeur - en pixels) qu'elle peut utiliser. Lors d'un accès à la page Web, le navigateur télécharge l'applette depuis un serveur et l'exécute sur la machine de l'utilisateur (le client). Les

	applettes diffèrent des applications dans le fait qu'elles sont dirigées selon un protocole de sécurité strict. Par exemple, bien que les applettes s'exécutent sur le client, elles ne peuvent pas lire ou écrire des données sur la machine du client. De plus, les applettes sont également limitées pour ne pouvoir lire et écrire des données que depuis le domaine les hébergeant.
Archive	Une disquette, une bande, ou un répertoire qui contient des fichiers qui ont été sauvegardés. Un fichier qui contient un ou plusieurs fichiers dans un format compressé.
Backdoor	Il s'agit d'une faille dans la sécurité d'un système délibérément laissé en place par des développeurs ou mainteneurs. La motivation n'est pas toujours négative ; quelques logiciels permettent à des techniciens de maintenance, via des comptes privilégiés, de prendre le contrôle à distance.
Chemin	Les directions exactes vers un fichier. Ces directions sont décrites d'habitude par arborescence, de haut en bas. La connexion entre deux points, telle le canal de communication entre deux ordinateurs.
Client de messagerie	Un client de messagerie est un logiciel qui vous permet d'envoyer et recevoir des messages (e-mails).
Cookie	Sur Internet, les cookies sont définis comme étant de petits fichiers contenant des informations sur les ordinateurs individuels qui peuvent être analysés et utilisés par des annonceurs publicitaires pour tracer vos centres d'intérêts et vos goûts. Dans ce milieu, la technologie des cookies est encore en développement et l'intention est de cibler directement ce que vous avez dit être vos intérêts. C'est une épée à double tranchant pour beaucoup de personnes parce que d'une part, c'est efficace et pertinent (vous voyez seulement des annonces vous intéressant) mais d'autre part, cela implique en réalité "le pistage" et "le suivi" d'où vous allez et de ce sur quoi vous cliquez sur Internet. Il y a naturellement un débat sur la vie privée et beaucoup de gens se sentent

	ainsi considérés comme un simple " numéro SKU " (vous savez, le code barres à l'arrière des produits). Bien que ce point de vue puisse paraître extrême, dans certains cas cette perception est justifiée.
Définition virus	La "signature" binaire du virus, utilisé par l'antivirus pour la détection et l'élimination du virus.
Disk drive	C'est une appareil qui lit et écrit des données sur un disque. Une unité de disque dur lit et écrit sur un disque dur. Un lecteur de disquette accède à des disquettes. Les lecteurs peuvent être soit internes (intégrés à un ordinateur) soit externes (intégrés dans un boîtier séparé que l'on connecte à l'ordinateur).
Evénements	Il s'agit d'une action ou d'une occurrence détectée par un programme. Les événements peuvent être des actions d'utilisateur, comme le clic sur un bouton de souris ou la pression d'une touche, ou des occurrences du système, comme l'analyse de la mémoire.
Extension de fichier	La partie d'un fichier, après le point final, qui indique le type de données stockées dans le fichier. De nombreux systèmes d'exploitation utilisent des extensions de fichiers, par exemple Unix, VMS, MS Dos. Elles comportent communément une à trois lettres (certains vieux OS ne supportent pas plus de trois). Exemples : "c" pour du code source en C, "ps" pour PostScript, "txt" pour du texte.
Fausse alerte	Se produit lorsqu'une analyse identifie un fichier comme infecté alors qu'il ne l'est pas.
Fichier journal (Log)	Un fichier qui enregistre les actions qui surviennent. BitDefender maintient un fichier journal contenant les chemins analysés, les dossiers, le nombre d'archives et de fichiers analysés, le nombre de fichiers suspects et infectés.
Heuristique	Méthode permettant d'identifier de nouveaux virus. Cette méthode d'analyse ne s'appuie pas sur des définitions virales spécifiques. L'avantage de l'analyse heuristique

	est de pouvoir détecter des variantes d'un virus existant. Cependant, cette méthode peut parfois occasionner de fausses alertes dans des programmes normaux.
IP	Protocole Internet - Un protocole routable de la suite de protocoles TCP/IP qui se charge de l'adressage, du routage IP et de la fragmentation et réassemblage des paquets IP.
Ligne de commande	Dans une interface en ligne de commande, l'utilisateur tape directement des commandes correspondant à des ordres de gestions.
Mémoire	Zone de stockage interne dans votre ordinateur. Le terme mémoire regarde le stockage des données dans les "chips" (composants), et le terme stockage regarde les disques. Chaque ordinateur a une certaine quantité de mémoire physique, appelée mémoire vive ou RAM.
Messagerie électronique	Courrier électronique. Il s'agit d'un service d'envoi de messages sur des ordinateurs via un réseau local ou global.
Mise à jour	Une nouvelle version du logiciel ou d'un produit hardware, destinée à remplacer une ancienne version du même produit. D'habitude, les installations de mises à jour vérifient si le produit initial est installé, sinon la mise à jour ne se fait pas. BitDefender comporte un module spécial pour la mise à jour. Ce module vous permet de chercher manuellement les mises à jour ou de faire la mise à jour automatiquement.
Navigateur	Raccourci pour navigateur internet, il s'agit d'un logiciel utilisé pour visualiser des pages Web. Les deux navigateurs les plus populaires sont Netscape Navigator et Microsoft Internet Explorer. Les deux sont des navigateurs graphiques, ce qui signifie qu'ils peuvent afficher aussi bien le graphisme que le texte. De plus, les navigateurs les plus modernes peuvent visionner les informations multimédia, y compris le son et la vidéo, bien qu'ils exigent des modules d'extension (plugins) pour certains formats.

Non-heuristique	Cette méthode d'analyse utilise les définitions spécifiques des virus. L'avantage de l'analyse non-heuristique est qu'elle n'est pas trompée par ce qui peut paraître un virus et ne génère donc pas de fausses alertes.
Objets menu démarrage	Tous les fichiers placés dans ce dossier s'ouvrent au démarrage. Par exemple, un écran de démarrage, un fichier son pour quand l'ordinateur démarre, un calendrier, des programmes, peuvent être placées dans ce dossier. D'habitude c'est un raccourci vers le fichier qui est mis dans le dossier, et pas le fichier.
Phishing	Action d'envoyer un email à un utilisateur en feignant d'être une entreprise connue dans le but d'obtenir frauduleusement des informations privées et qui permettront d'utiliser l'identité du destinataire du mail. Cet email oriente l'utilisateur vers un site Web où il lui est demandé de mettre à jour des informations personnelles, comme ses mots de passe, son numéro de carte de crédit, de sécurité sociale ou de compte en banque, que les véritables entreprises connaissent déjà. Ce site Web est bien sûr totalement factice et n'a pour objectif que de voler les informations de l'utilisateur.
Port	Une interface de l'ordinateur à laquelle vous pouvez connecter un périphérique. Les PCs comportent plusieurs sortes de ports. A l'intérieur, il y a quelques ports pour la connexion des disques, cartes vidéo. A l'extérieur, les PCs ont des ports pour connecter des modems, imprimantes, souris et autres périphériques. Dans des réseaux TCP/IP et UDP, un point final pour une connexion logique. Le numéro du port identifie son type. Par exemple, le port 80 est utilisé pour le trafic HTTP.
Programmes empaquetés	Un fichier comprimé. Beaucoup de plates-formes et applications contiennent des commandes vous permettant de comprimer un fichier pour qu'il occupe moins de mémoire. Par exemple, imaginons que vous avez un fichier texte contenant dix caractères "espace vide". Normalement, cela nécessite 10 octets.

Pourtant, un logiciel qui comprime les fichiers remplace la série d'espaces par un caractère spécial série d'espaces suivi du nombre d'espaces remplacés. Dans ce cas, les dix espaces nécessitent seulement 2 octets. C'est juste une technique de compression, il y en a une multitude.

Script

Autre terme pour macro ou fichier batch, un script est une liste de commandes qui peut être exécutée sans intervention utilisateur.

Secteur de boot

Un secteur au début de chaque disque qui identifie l'architecture du disque (taille des secteurs, etc). Pour les disques de démarrage, le secteur de boot contient aussi un programme qui charge la plate-forme.

Spam

Message électronique ou envoi de messages souvent répertoriés comme des emails « non sollicités ».

Spyware

Tout type de logiciel qui récupère secrètement les informations des utilisateurs au travers de leur connexion Internet sans les avertir, généralement à des fins publicitaires. Les spywares sont généralement cachés dans des logiciels shareware ou freeware qui peuvent être téléchargés sur Internet. Cependant, la majorité des applications shareware ou freeware ne comportent pas de spyware. Après son installation, le spyware surveille l'activité de l'utilisateur sur Internet et transmet discrètement des informations à une tierce personne. Les spywares peuvent également récupérer des informations sur les adresses mail, les mots de passe ou même les numéros de cartes de crédit.

Leur point commun avec les Chevaux de Troie est que les utilisateurs les installent involontairement en même temps qu'un autre produit. Une de manière les plus classique pour être victime de spywares est de télécharger des logiciels de partage de fichiers (Peer to peer).

En plus des questions d'éthique et de respect de la vie privée, les spywares volent aussi les ressources de l'ordinateur de l'utilisateur en utilisant de la bande passante lors de l'envoi d'information au travers de sa connexion Internet. A cause de cette utilisation de la mémoire et

	des ressources du système, les applications qui fonctionnent en tâche de fond peuvent aller jusqu'à entraîner des plantages ou provoquer une instabilité globale du système.
System tray (Zone de notification)	Introduit avec Windows 95, le system tray se situe dans la barre de tâches Windows (à côté de l'horloge) et contient des icônes miniatures pour des accès faciles aux fonctions système: fax, imprimante, modem, volume etc. Double cliquez ou clic droit sur une icône pour voir les options.
Téléchargement	Copier des données (généralement un fichier entier) d'une source principale à un dispositif périphérique. Le terme est souvent utilisé pour décrire le processus de copie d'un fichier d'un service en ligne vers son ordinateur. Le téléchargement peut aussi se référer à la reproduction d'un fichier d'un serveur de réseau vers un ordinateur sur le réseau.
TCP/IP	Transmission Control Protocol/Internet Protocol - Un ensemble de protocoles réseau utilisés largement sur Internet assurant la communication entre des réseaux interconnectés avec divers architectures hardware et diverses plates-formes. TCP/IP inclut des standards pour la communication des ordinateurs et des conventions pour la connexion des réseaux et le routage du trafic.
Trojan (Cheval de Troie)	Un programme destructif qui prétend être une application normale. Les Trojans ne sont pas des virus et ne se repliquent pas, mais peuvent être tout aussi destructifs. Un des types les plus répandu de Trojans est un logiciel prétendant désinfecter votre PC (mais au lieu de faire cela il l'infecte). Le terme provient de la fameuse histoire de l'Iliade écrite par Homère, dans laquelle les Grecs font un cadeau de "paix" à leurs ennemis, les Trojans, un immense cheval en bois. Ce n'est qu'après avoir fait entrer le cheval dans leur ville qu'ils se rendent compte que le cheval est plein de soldats grecs, qui ouvrent les portes de la ville, permettant aux attaquants de capturer Troie.

Ver Internet	Un programme qui se propage tout seul en réseau, se reproduisant au fur et à mesure qu'il se propage. Il ne peut pas s'attacher aux autres programmes.
Virus	Un programme ou morceau de code qui est chargé dans votre ordinateur sans que vous le sachiez et fonctionne contre votre gré. La plupart des virus peuvent se répliquer. Tous les virus sont crées par des personnes. Un virus simple peut faire une copie de lui-même très vite et sans arrêt et est relativement facile à créer. Même un virus simple comme celui décrit est dangereux puisqu'il remplit vite la mémoire et bloque le système. Un virus plus dangereux encore est capable de se transmettre via un réseau par exemple.
Virus de boot	Un virus qui infecte le secteur de boot d'une disquette ou d'un disque dur. Une tentative de démarrer depuis une disquette infectée avec un virus de boot rendra le virus actif en mémoire. Chaque fois que vous démarrez votre système depuis ce point, vous aurez le virus actif en mémoire.
Virus Macro	Un type de virus codé sous la forme d'une macro intégrée dans un document. Beaucoup d'applications, telles Microsoft Word et Excel, supportent des langages macro. Ces applications vous permettent d'intégrer une macro dans un document, et de le faire s'exécuter chaque fois que le document est ouvert.
Virus polymorphique	Un virus qui change de forme avec chaque fichier qu'il infecte. Comme ils n'ont pas une forme unique bien définie, ces virus sont plus difficiles à identifier.